



CENTRE *for* DOCTORAL TRAINING *in*  
**CYBER  
SECURITY**



**CDT Technical Paper**

**01/17**

**Can improved transparency reduce  
supply chain risks in cloud computing?**

**Olusola Akinrolabu**



**Can improved transparency reduce supply  
chain risks in cloud computing?**

**June 2016**

**OLUSOLA AKINROLABU**

## Table of Contents

<b>0. Abstract .....</b>	<b>3</b>
<b>1. Introduction .....</b>	<b>3</b>
<b>2. Literature Review/Background .....</b>	<b>6</b>
Figure 1: A typical SaaS delivery chain .....	12
<b>3. Methodology.....</b>	<b>12</b>
<b>4. Results and Discussion .....</b>	<b>15</b>
<b>4.1 Introduction .....</b>	<b>15</b>
<b>4.2 Case study .....</b>	<b>16</b>
Figure 2: Payfruit cloud services supply chain .....	16
<b>4.3 Interviews.....</b>	<b>20</b>
<b>4.4 Risk Assessment .....</b>	<b>23</b>
Figure 3: CSPs that have an established procedure for contracts .....	25
Table 1: Risk assessment of cloud providers .....	27
<b>4.5 Cloud provider comparison .....</b>	<b>27</b>
Table 2: Detailed description of CSP comparison criteria. ....	29
Table 3: Comparison of 25 SaaS providers taken from Cloudscape .....	30
<b>4.6 Supply chain questionnaire to verify CSP comparison result .....</b>	<b>33</b>
Figure 4: Cloud knowledge of the MBA respondents.....	34
Figure 5: Benefit vs. Risk of cloud supply chain. ....	35
Figure 6: Assessment of CSPs by MBA respondents. ....	37
<b>5. Conclusion and Future work .....</b>	<b>38</b>
Acknowledgement .....	41
<b>References .....</b>	<b>42</b>
<b>Annexe A – Risk Assessment questionnaire.....</b>	<b>46</b>
<b>Annexe B – Non-technical supply chain questionnaire.....</b>	<b>46</b>
<b>Annexe C - Description of the 25 compare SaaS providers.....</b>	<b>46</b>

## Abstract

As organisations move sensitive data to the cloud, their risk profile increases, due to the integrated supply chain utilised in cloud computing. The risk is made visible in situations where a cloud offering is federated, with customer data located in multiple datacenters, under the control of multiple providers and sub-providers in different jurisdictions. This problem is further exacerbated by the disposition of cloud providers to keep details of suppliers, data location, architecture and security of infrastructure confidential from the cloud customers. As such, the shallowness of transparency amongst cloud providers makes it difficult for customers to assess the risk of cloud adoption. In this study, we report on our research into finding out how much customers know about their supply chain. We evaluate the transparency of cloud providers based on their published information and determine the resultant risk of limited visibility of the supply chain. In the course of the research, we identified eight transparency features, which, at a minimum, cloud providers should make available to their current or prospective customers, which we argue had no adverse impact on the competitiveness or profitability of the provider. The study concludes that ultimately, cloud supply chain transparency remains a customer-driven process.

*Keywords-* Cloud computing, supply chain, transparency, trust, risk, ERM.

## 1. Introduction

Cloud computing is an innovative shift from the traditional hardware outsourcing and independent software provider models. The cloud technology allows for the provisioning of Information Technology (IT) resources “as a service”, and offers this cloud service on a pay-per-use model (Leimeister et al., 2010; Sunyaev & Schneider, 2013). The utilisation of cloud services affords organisations, especially the smaller firms, access to compute-intensive applications, hardware resources with no upfront cost, a platform for innovation and IT scalability (Marston et al., 2011). Due to the use of distributed computing in cloud computing, there exists, an inherent concept of a supply chain where each member of the chain does what they know how to do best (Pohlman, 2010). The five characteristics of cloud computing (on-demand self-service, broad network access, resource pooling, rapid elasticity & measured service), as articulated in the NIST definition, further highlights the importance of supply chain in cloud offerings (Kaliski-Jr & Pauley, 2010). Likewise, the IT infrastructures that host cloud services can be hosted with multiple processors and subcontractors along a cloud chain, who belong to different legal entities and may be located in various jurisdictions. Besides, a layered cloud service involving multiple sub-providers will invariably pose a higher risk than a service hosted by a single provider (Weber & Staiger, 2014). Therefore, the risk of adopting a cloud service increases with the degree of in/outsourced hosting that makes up the service.

When organisations move their business processes to the cloud, their risk profile changes, and becomes a combination of their risks and a subset of their cloud service provider (CSP) risk, leading to many unknowns (Cayirci et al., 2014; Chan et al., 2012). Without sufficient management insight (due diligence) into the procurement of cloud services, a small investment in a BAU cloud application could have a significant impact on an organisation’s security posture (Chan et al. 2012). For

example, the human resources (HR) department of a large corporation independently deciding to leverage a cloud-based HR system and storing staff member's personally identifiable information (PII) outside the organisations trust boundary, exposes the business to an increased risk of data loss or malicious attack. The abstraction of the cloud, the dynamism of the supply chain and the fundamental lack of transparency of cloud providers further exacerbate the risk organisations face when they adopt cloud computing. Felici and Pearson (2015) assert the need for accountability in the cloud and list four main factors that contribute to making accountability difficult, two of which are the potential weak links in the dynamically formed supply chain and shallowness of transparency and verifiability. The lack of visibility into cloud supply chain makes it difficult to determine how data is treated when in the hands of sub-providers, given the limited insights customers have into sub-provider location, compliance, jurisdiction and processes (Raj Samani, 2011). To adequately assess cloud risks, organisations require an awareness or visibility of their third party risks. However, historically, providers have been circumspect about supply chain visibility for the genuine risk of industrial espionage, sabotage, malicious attack or even reputational damage (New & Brown, 2012). As such, there seems to be a distinct lack of supply chain transparency amongst CSPs, and this is setting back cloud adoption.

In this paper, we investigate the extent of supply chain information CSPs share with their customers and suggest steps that providers can take to improve the transparency of their supply, to allay the growing concern amongst cloud consumers, who leverage cloud resources for their business-as-usual (BAU) and strategic goals. We argue that since the purpose of every cloud supply chain is to achieve high quality and responsive service offered at a low cost to the customer, the goal could be facilitated through increased visibility into the vulnerability of the chain, which helps to foresee challenges and enable proactive response, increasing both efficiency and profitability. According to ISACA & CSA (2015) & Lynn et al. (2013), organisations around the world, despite their adoption of cloud services, worry over the location, integrity, portability, scalability, security and privacy of their data. Previous studies into the cause of limited transparency in computing technologies including the cloud, found the cost of provenance to be a major obstacle. Fisher et al. (1997) put forward the view that investing in supply chain efficiency for innovative and short lifecycle products, leads to a decrease in margin. Although the research of Pearson et al. (2012) identified the general desire for secrecy amongst CSPs especially those involved in the development of encryption-based proprietary security, New & Brown (2012) were able to establish a case for the genuine risks that can result from supply chain transparency. For example, the competitor of a Software-as-a-Service (SaaS) provider could clone their business model by using the same Infrastructure-as-a-Service (IaaS) provider and undercut their price by, say, twenty percent. Many providers of innovative technologies fear that greater visibility into their chain could reduce their exclusivity or set back their market position, especially in the event of continuous supply chain disruption (New & Brown, 2012). While we recognise the cost implication and risk of espionage that is synonymous with the transparency of the supply chain, we investigate the level of information customers require to be able to assess their risks adequately and implement controls to protect their company sensitive information and intellectual property.

Transparency allows customers to verify that their trust in the CSP isn't misplaced (Vijayan, 2015). According to Kaliski-Jr and Pauley (2010), an increased level of

trust improves disclosure, reduces the demand for legislation, and reduces perceived risk. Albert S. & Rajeev (2015) hold the view that improved visibility of the supply chain helps customers to determine the trustworthiness of a cloud service a priori, based on its profile and security assurances. Transparency also encourages an alliance between customers and provider, allowing CSPs to focus their resources on providing services their customers want, and likewise benefitting more from an increased market share (Wisner et al. 2008). Gavan Egan, vice-president of Verizon Terremark Europe, said, "Transparency is the biggest challenge in moving to the cloud and not security" (Ashford, 2013). Central to human nature is the concept of increased trust leading to greater transparency. The cloud ecosystem requires a higher level of assurance that supersedes the traditional security assurance obtainable from audits and certifications. Werff et al. (2014) highlight the advantage of cloud trust built on the knowledge of CSPs processes, architectures, and visible controls over the trust based on pure calculation. The cloud customers, who are referred to under the European Union (EU) data protection directive (DPD) as the data controllers, are ultimately responsible for the data they put in the cloud since they only outsource the control of such data to their cloud provider (Werff et al., 2014). Since it is the responsibility of the customer to decide how their data is to be processed, they are also held liable for a breach of that data, according to the EU DPD. Whereas, the CSP (data processor) who processes the data on behalf of the controller is subject to a lesser burden (Weber & Staiger 2014). The use of cloud infrastructure and the cede of control to CSP can lead to security gaps, particularly when the CSP's SLA does not offer a commitment to cover such gap in security defences (ENISA, 2009). Furthermore, Dziminski and Gleeson (2015) were able to identify how a provider or sub-provider could double as a data processor and a data controller, in situations where they act in an inconsistent manner to the customer's instruction regarding the use of their data. For example, a cloud provider of social network service running advertisement against a customer's uploaded personal data. To tackle such issue, they argue that cloud contracts should have a chain of contractual responsibility where agreement between the CSP and customer is capable of being cascaded to sub-providers involved in the service.

According to Cloud Security Alliance (CSA), insufficient due diligence is among the top threats of cloud computing (Cayirci et al., 2014). It is a widely held view that increased visibility into the vulnerability of the supply chain enables customers and providers to foresee challenges and implement proactive response, while increasing both efficiency and profitability. This visibility concern together with customers' inability to monitor Service Level Agreements (SLA), CSP's dependence on a complex supply chain, and the lack of assurance on data integrity adds to the long list of cloud risks (Werff et al., 2014). Our goal is to investigate how much cloud providers know about the supply chain of their cloud service and what they are willing to share with their customers. It is our aim to establish how providers can best present supply chain information to their customers, and identify if customers want supply chain transparency or just need an assurance.

The novelty of this paper is to examine what information CSPs currently share with their customers, its effect on cloud adoption, and how CSP transparency can be improved. According to Boyens et al. (2015), cloud supply chain risks are associated with an organisation's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed. Cloud customers who have put aside their long-held reservations on security and privacy, to bow to the

advantages of the cloud, are now seen to challenge their CSPs to be more transparent (Vijayan, 2015). Thus, we aim to investigate the amount of information readily available on cloud provider websites and carry out a systematic comparison among twenty-five SaaS vendors. Likewise, we sought to find out from a few providers what they know about their supply chain and how much they are willing to share with their customers. Finally, we assess a few of our interviewees based on the supply chain information they possess about their cloud service operation

To help us understand what CSPs think of supply chain transparency, we developed a fictional story of a Software-as-a-Service (SaaS) provider, who suffered a downtime for approximately four hours as a result of a power outage at their CSP's Internet service provider (ISP). We requested respondents to assume they were the management of the SaaS provider who was holding a post-incident meeting with their IaaS provider about the outage. We asked the respondents to help give answers to two questions namely: i) what questions should the SaaS providers ask their infrastructure provider? ii) How much information on its supply chain should the CSP is willing to share? Also, we carried out a mini risk assessment of the cloud providers, to determine their risk profile resulting from their level of supply chain awareness. Lastly, we interviewed a few cloud providers to discover more about their supply chain and get their views on transparency in cloud computing.

The remainder of the paper is structured as follows: Section 2 reviews the literature concerning supply chain risks, transparency and cloud computing. Section 3 then describes our research question (RQ) and methodology. Section 4 continues by presenting our risk assessment result and discussion on our findings. Finally, we conclude the paper in Section 5 and present ideas for future research.

## **2. Literature Review/Background**

There appears to be very little studies that have directly addressed the effect of supply chain transparency in reducing cloud computing risks. Although, we are aware of the efforts of leading organisations such as CSA, National Institute of Standards and Technology (NIST) and European Network and Information Security Agency (ENISA), who have published studies, surveys and recommendations addressing cloud computing risks. The CSA in trying to address the due diligence risk, which ranks as one of the notorious nine cloud computing threats developed the Consensus Assessments Initiative Questionnaire (CAIQ) (Cayirci, 2015; Pohlman, 2010). The CAIQ is a due diligence questionnaire that allows CSPs to demonstrate their compliance to potential customers through the documentation of their implemented security controls. Cloud customers use the CAIQ to build assessment processes for CSP, and it helps them to understand the security controls of specific cloud offerings (Cayirci et al., 2014). NIST define security controls as "the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information" (Boyens et al., 2015). Despite the usefulness of CAIQ in helping organisations formulate the right questions to ask prospective providers, the process is still slow, painful and discriminatory in that a small organisation submitting a questionnaire to a big cloud service provider can expect little cooperation, let alone answers.(Raj Samani, 2011).

Before we progress any further, we should describe some of the core terms of our work in greater detail, beginning with cloud computing. Amongst the plethora of definitions for cloud computing, we present that of Leimeister, et al. (2010), who defined cloud computing as an “IT deployment model, based on virtualization, where resources, in terms of infrastructure, applications and data are deployed via the internet as a distributed service by one or several service providers”. These services are scalable, on-demand and can be priced on a pay-per-use basis”. Wisner et al. (2008) define a supply chain as the series of companies that make products and services available to consumers, including all the functions enabling the production, delivery, and recycling of materials, components, end products and services. Also, according to FT Lexicon (n.d.), supply chain transparency captures the extent to which information about the companies, suppliers and sourcing locations is readily available to end-users and other businesses in the supply chain. Lastly, a risk is defined in ISO 27005 (2011), as the effect of uncertainty on objectives. Wisner et al. (2008) also describe supply chain risk as the likelihood of an internal or external event that causes a disruption or failure of supply chain operations, causing potential reductions in service levels, product quality, and sales, with an increase in costs.

Previous researches into cloud computing risks and supply chain have touched on SLA, jurisdiction, compliance, data privacy, trust, traceability (provenance), accountability, transparency and standards. We would highlight a few of these works and identify their relation to our research. Cloud computing risks range from high, medium and low risks, and these risks are dependent on organisation, cloud model and service provider offering. In strategic alliances, such as the cloud service supply chain, there are two broad categories of risk: relational risk, which is where the partner is not operating in good faith, and performance risk, which is the risk of unsatisfactory business performance (Das & Teng, 2001). Some of the typical cloud computing risks include i) disruptive force –changing the way organisations do business; ii) multi-tenancy liability- organisation is impacted by mistakes of CSP or other tenants; iii) lack of transparency; iv) high-value cyber attack targets- the consolidation of multiple organisation increases the likelihood of attacks and v) risk of data leakage (Chan et al., 2012). Although, majority of these risks are not likely to be mitigated by contractual clauses with the CSP, many cloud customers, particularly SMBs, in embracing the cloud's economies of scale and flexibility advantages, end up blindly trusting the CSP and accepting the risk to run their entire enterprise in the public cloud due to the small up-front capital investment requirements.(Chan et al. 2012; Gadia 2011).

Felici & Pearson (2015) identified the effect of multi-tenancy, abstraction, automation, data duplication, data access from multiple locations and sub-processing as positive cloud features that could potentially have an adverse effect on data protection. Weber & Staiger (2014) in observing the complex liabilities of the cloud, emphasise the increased risk associated with a layered cloud service involving multiple sub-providers when compared to another with a single provider. This complex service provision eco-system may not be visible to an enterprise outsourcing their data processing to a CSP (Pearson et al. 2012). Cayirci (2015) explored the complexity involved with CSPs complying with the legal systems when they deliver cloud services over the Internet to global customers. They identify the frustrations and the near impossibility of cloud providers to satisfy all the applicable laws in these jurisdictions, which is a reason for some deciding not to comply or avoid doing

business in some jurisdictions. Microsoft (2015) in identifying the top five deliverables customers want from their CSP, explained how the complexity and scope of standards and regulations continue to evolve with the increase in an organisation's cloud adoption. It becomes more challenging for an organisation to be assured of its compliance with regulations, as its data moves within the cloud supply chain. Pearson et al. (2012) recommend the application of a “chain of accountability” whereby members of a cloud ecosystem ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs.

According to Weber & Staiger (2014), the move to the cloud consists of two decisive factors: risks associated and benefits to be gained. Chan et al. (2012) recognise the need for organisations to account for cloud computing risks in their enterprise risk management (ERM) programs. They recommend that as a prerequisite for cloud adoption, organisations should have a strong governance model, a sound reporting structure, an understanding of internal IT skills and most importantly a clearly defined risk appetite. The effectiveness of risk management strongly depends on the degree to which it succeeds in becoming a part of an organisation's culture (ENISA, 2006). It should be an endlessly re-occurring process with phases that if implemented enables continuous improvement in performance. Along similar lines, CERT-UK (2015) uses examples of security compromises to illustrate the need for a broad, inclusive approach to risk management within a supply chain, stressing that it helps organisations to map their cyber security dependencies and vulnerabilities. However, ENISA (2006) identified the little awareness of risk management activities, in particular among the SMBs, who they claim some do not even have an ERM to govern their risks. Some other factors identified in other works of literature, as the hindrances to ERM are the absence of a common risk vocabulary, the inadequate information sharing across the supply chain, inappropriate or non-existent business resilience strategies and lack of interoperability of ERM tools to mention a few (CERT-UK, 2015; ENISA, 2006). The best-practice situation for cloud adoptions is when an organisation's management use ERM framework to identify the ideal configuration of cloud solution options (Chan et al., 2012).

Felici & Pearson (2015) recognise an in-depth connection between accountability, trust and risks, whereby accountability enhances trust and trust help change consumers and providers perception of risk. The ISO21000 highlights transparency and inclusivity as part of the principles for a successful risk management (Verbano & Venturini, 2013). According to CERT-UK (2015), cyber security risk management within the supply chain is primarily an issue of trust. Wisner et al. (2008) in identifying obstacles that often prevent the integration of supply chain listed the lack of trust, silo mentality and lack of visibility. According to ISACA & CSA (2015), this trust is built mainly on provider's reputation and through visible controls, the service provider has implemented. This trust can be established based on performance, predictability and helpfulness of the CSP (Werff et al. 2014). The A4Cloud in their research work, focus on accountability as the most crucial prerequisite for the control of corporate and private data processing in the cloud, and they claim CSPs should be held accountable for how they manage personal, sensitive and confidential information in the cloud (Pearson et al., 2012). One of the ways of achieving this trust could involve CSPs providing customers with greater transparency and control over how their data is processed in the cloud. The level of trust to place on a CSP is one of the most debated topics when customers assess cloud services and a few frameworks

have been developed for assisting customers. Garg et al. (2012) developed the SMI framework for ranking CSPs using attributes such as accountability, transparency, and security. Also, Werff et al. (2014) propose the utilisation of a nutrition label concept to provide clarity and greater consumer access to CSP information, while Lynn et al. (2013) suggest that cloud providers could use of trustmarks as a way of providing assurance.

Trust is essential for cloud survival as it fosters sharing of valuable information within the supply chain. Trust is fragile; considering the amount of time it takes to build and the no time to tear down. Improved communication within the supply chain and transparency into the adequacy of the internal controls provides trust in operation confidence and adequate understanding of residual risk (ISACA & CSA 2015). Das & Teng (2001) establish the linkage of trust and control with risk when dealing with strategic alliances. They propose that both trust and control can reduce perceived risk but not “objective” risk, especially when the risk is inherent in a given situation. For example, a cloud customer who trust their CSP, and have been given full control over their data, will have a low-risk perception for their cloud arrangement, but that does not take away the inherent risk of data loss or supply chain failure. Sheppard and Tuchinsky (1996) suggest that in organisational or professional relationships, there are three types of trust – deterrence or rule-based, knowledge-based and identity-based. Sheppard and Tuchinsky (1996) argue that there is a sequence in which trust develops between partners or within an organisation. Similarly, Conley (2012), identifies three levels of trust asserting that deterrence-based trust which relies on contracts, policies and laws to provide the boundary of trust is the first stage in a trust relationship. Followed by the knowledge-based trust, which results from having enough experience and interaction over a period with the partner and there has been a consistent display of trustworthy behaviour. Conley (2012) notes that the identity-based trust is the most intimate level of trust, and it results in increased level of transparency and vulnerability with the partner or individual. Identity-based trust signals the loyalty of the parties to one another and is the basis of most literature definitions of trust. For example, (Rousseau et al. 1998) defined trust as “ the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trusting party, irrespective of the ability to monitor or control the trusted party”.

According to CPNI (2015), the awareness or visibility of third-party risks is the key to effective risk management. The integrated supply chain in cloud computing, whereby standardised cloud services are built on existing sub-provider services, calls for an increased transparency to help identify potential failure or disruption points in the supply chain, and establish a likelihood/probability of their occurrences. Wisner et al., (2008) observe the dynamic boundaries of supply chain and the difficulty of providers to coordinate supply chain beyond the 2nd tier, while Tom Ridge, CEO of risk management firm Ridge Global, is of the opinion that supply chains especially those involving multinational firms, need to be vetted down to the second, third, and fourth tiers (Wisner et al., 2008). However, Boyens et al. (2015) and New & Brown (2012) share an important premise concerning the increase in the cost of doing business with providers that allow increased level of visibility into their security and supply chain practices. Another important argument put forward against visibility, is one of liability, whereby you become more liable the more you know about your supply chain (New, 2009). Bhensook & Senivongse (2012) in their design of system

architecture for scoring cloud providers argue that although cloud providers need to build consumer trust by disclosing sufficient information about security design, practices, and procedures that will protect consumer data, the providers still have to protect critical security information for overall governance. With the global drive towards *Anything-as-a-Service*, Cayirci (2015) propose the idea of CSPs offering Security-as-a-Service, as a way of getting them to provide transparent security services where the actual controls they will enforce together with the metrics for measurement can be clear to customers. For many customers, knowing and controlling the location of their data can be an important element of data privacy, compliance, and governance (Microsoft, 2015).

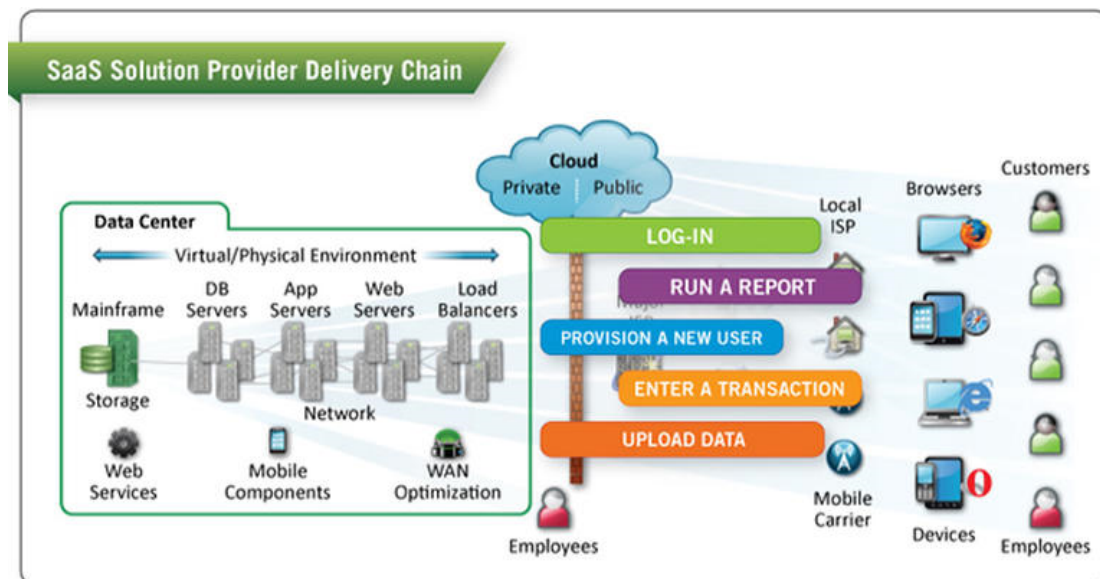
Cloud risks are associated with the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the cloud service (Boyens et al., 2015). Cloud computing risk is further exacerbated by the high rate of technological change and the dynamically complex supply chain network. According to Chopra & Sodhi (2004), most companies develop plans to protect against recurrent, low-impact risks in their supply chains, and all but ignore the high-impact, low-likelihood risks. For example, when big cloud providers are asked about what will happen should they lose one of their primary datacenters to terrorism, the response they give leads one to believe such risk is not in-scope. It is pertinent for organisations whose critical data reside in the cloud to develop a robust threat model to help identify and prioritise the supply chain risks (Charney & Werner, 2011). Chopra & Sodhi (2004) present the view that understanding the variety and interconnectedness of supply chain risks would assist risk managers in developing a tailor-balanced and effective risk-reduction strategy for their organisations, but argue that perhaps the biggest challenge companies face is mitigating supply-chain risks without eroding profits. According to Charney & Werner (2011), any framework needed to mitigate supply chain risk must promote transparency by all parties.

Boyens et al.(2015) demonstrate how managing ICT supply chain risks could be a complex, multifaceted undertaking that requires a coordinated effort across an organisation. Risk management involves identifying and understanding potential risks, determining the likelihood and consequences of each risk, ranking the risks according to their weighted costs, and then finally implementing risk mitigation plans for the risks deemed unacceptable (Wisner et al., 2008). In Leimeister et al. (2010) analysis of existing supply chain risk management (SCRM) literature, they identified the four key elements for managing supply chain risks as: (1) risk identification; (2) risk assessment; (3) risk mitigation; and (4) responsiveness to risk incidents. Stress testing and scenario planning using "what-if" scenarios have been identified as an important component in assessing supply chain risks (Chopra & Sodhi, 2004; Schlegel & Trent, 2012). Schlegel & Trent (2012) recommends going through multiple iterations of the situation until it becomes statistically significant. Organisations need to ask questions such as "What might happen if a particular cloud provider could not deliver for a month?" (Chopra & Sodhi, 2004). Kaliski-Jr & Pauley (2010), make a case for "on-demand" risk assessment just in the same manner in which cloud service is delivered: as a service. They argue that this would address the recursive nature of cloud computing, providing the customer with a way to assess providers as their data transits through its cloud environment. The primary challenge with assessing the risk of cloud computing stems from the fact that the data that is needed to estimate the impact and likelihood of risk scenarios or events are either

unavailable or inadequate. Typical examples of such information are experience or incident reports, market research and analysis, reliable practices, international standards or guidelines (ENISA 2006). From our check, there is no publicly available and statistically acceptable quantitative research carried out on cloud computing risks, due to the inadequacy of numerical data.

For the sake of discussion, we would argue that supply chain transparency in cloud computing is not black and white. The decision about the extent to which cloud providers make their supply chain network transparent to their customers has a strategic significance, which might only be addressable, at board level (New & Brown, 2012). According to Hofstede (2002), supply chain information should not be provided unless requested, because knowing what information the customer wants is a precondition for transparency. Along similar lines, Fischer-Hübner et al. (2014) present the view that complex supply chain information can be provided in layers, where a high level is provided first, and further details are made available to customers who probe for more information. Data transparency alone is not enough, as there is not much value with been packed with too much data when such data is inconsistent or cannot be understood by the recipient (Akkermans, 2004). Hofstede (2002) puts forward the view that transparency is about effortless access to information and the quality of such information is an essential element of transparency. Lamming et al. (2002) propose that the information sharing within a supply chain must be reciprocal, selective, and justified but not necessarily symmetrical. In Lewis et al. (2014) research into cyber security information sharing, they acknowledge the positive impact of information share and the potential increase in risk exposure as a result, but they were able to identify conditions under which stakeholders in a supply chain were happy for information to be shared. (Lamming et al. 2002) points out that in reality, rather than being simply opaque, translucent, or transparent, supply relationships are likely to contain elements of all three characteristics, in a variety of locations at different times.

Two important themes emerge from the studies discussed so far; there is an inherent risk in cloud computing due to its dynamically complex supply chain, and also, the process of managing cloud computing risks can be improved through visible controls and improved transparency. Organisations adopting cloud computing, therefore, need a broad and inclusive ERM to accommodate the risks associated with the cloud. In our study, we take a look at the nature of information customers need to have about their CSP and its' supply network that can assure that the risk of adopting the cloud service can be operationalized. Likewise, we investigate the level of information on the supply chain that a sample of cloud providers currently share through their websites and how much they are willing to tell their prospective or current customers if probed for details.



**Figure 1:** A typical SaaS delivery chain (*Image Source: Compuware*).

### 3. Methodology

According to a recent study conducted by KPMG, they claim that the question on cloud computing is no longer: "How do I move to the cloud?" instead, it is "Now that I'm in the cloud, how do I make sure I've optimised my investment and risk exposure?" (Microsoft, 2015). Cloud computing is hard to disregard, particularly due to its benefit of economies of scale through volume operations, pay-per-use through utility charging and speed to market through componentization, which is of immense benefits to SMBs (Zhang et al., 2010). However, each cloud delivery model has some associated security risks, which varies based on the sensitivity of information assets, cloud architectures and security controls (Zhang et al., 2010). As earlier mentioned, the cloud security alliance's attempt at mitigating the insufficient due diligence risk through the use of CAIQ also tries to address the cloud supply chain risks. However, the success of the CSA CAIQ is limited to the about two hundred cloud vendors who signed up for the assessment out of the thousands of CSP around the world, with many providers claiming that they provide the information requested in the CAIQ in different forms and platforms already.

Our methodology to address the effect of transparency in reducing cloud supply chain risk was to engage in a field research. Qualitative methods (case study, questionnaires and interviews) were chosen to allow for a deeper insight into supply chain risks as we get to look at the issues from different perspectives, including both customer and providers in our study. We set out to determine how providers could offer a more transparent service to assist customers with mitigating their risks, while still maintaining their intellectual property and competitive advantage. Our research adopted the use of a case study, as it is a well-established approach to explorative investigation. We developed the case study for a fictitious company (Payworq) who experienced an outage due to their CSP's Internet Service Providers (ISPs) service failure. The questions that followed the case study contained aspects of our four main research questions, which are as follows:

1. What information should cloud customers ask CSP about its supply chain?

2. How much should CSP be willing to share with their customers?
3. What are the risks of customers not knowing enough about the supply chain?
4. How can transparency be improved in cloud computing?

As a supplement to our case study, we chose to interview cloud providers on their thoughts on supply chain transparency and its associated risk in cloud computing. The Cloud Expo event at the Excel Centre in London between the 12th and 13th of April, 2016, provided us with the opportunity to interact with a broad range of cloud providers. Before this occasion, we had made several attempts to discuss with individual cloud providers but were relatively unsuccessful. In preparing for the Cloud Expo, we looked into about 40 of the exhibitors, with a view of getting familiar with their cloud offering, their hosting infrastructure, partners and their general disposition to transparency. Most of the research we carried out on these firms was through their website and publicly available information, using Google search engine. As one would expect, the cloud providers were not all available to be interviewed, and a proportion of those that gave us an audience could only speak with us for about 10-15 minutes. Our plan was to get participants to talk to us in a quiet area, outside their organisations stand, but on most occasions, the interviewee's preference was to remain at their stand. Wherever we got an audience, we made sure to speak to the most technical representative of the firm who understood the cloud business and its complexities, a phenomenon Myers & Newman (2007) refer to as the Elite bias. There was also an evident lack of trust when we initially approached most of the interviewees, but our introduction as academic researchers and our ability to demonstrate knowledge of the research topic was enough to win them over.

Since our interview was for a qualitative research and because of the need to establish a social context, we adopted the dramaturgical model, which proved to be positive with our participants (Myers & Newman, 2007). We took the time to introduce ourselves, explain the purpose of the interview, ask and discuss the key questions and close out the interview with an offer to provide feedback to each respondent. Those interviewed were made up of SaaS, PaaS and IaaS vendors who either owned their hosting infrastructure or partnered with one of the top four cloud IaaS providers, named by Li et al. (2011) as Amazon Web Services, Microsoft, Google and Rackspace. Of the 40 exhibitors we approached, 15 of them granted us an audience, with the majority of the interview conducted on the promise of anonymity. The interviewees were made up of CEOs of start-up CSPs, technical directors and business development executives representing service providers, cloud brokers and Cloud equipment manufacturers. As the interview proceeded, we took notes and on two occasions, with permission from the interviewee, we audio-recorded the interview. The semi-structured nature of the research also enabled us to engage the cloud providers in further conversations around their cloud offering and supply chain while also giving us an opportunity to assess their transparency. In our discussions with the interviewees on their cloud offering, we treated this subject as sensitive and refrained from accusing them of any wrongdoing, as we know from Raymond & Renzetti (2015) research, this could undermine our research and lead to the withdrawal of the interviewee from the process.

In addition to the interview, some of the cloud providers were happy to contribute further to our research by way of carrying out a mini risk assessment of their cloud service supply chain. The design of the risk assessment questionnaire allowed us to

assess each organisation's risk based on their knowledge of their cloud service supply chain together with the processes and procedures they undertake to keep their cloud risks under control (see Annexe A for Questionnaire). The questions were written in a 5-point Likert scale format, and the participants were asked to choose the option that was most applicable to them from the options (*Yes, somewhat, No, complicated and, not applicable*). The questionnaire contained questions that we adapted from industry and academia research and guidance documents including the Control Objectives for Information and Related Technology (COBIT) framework, CSA CAIQ and the research of (Kleindorfer & Saad, 2010). Each of the participants in the risk assessment was requested to put down their email address beneath the form if they were interested in receiving feedback from our assessment of their organisation. Furthermore, we approached a few of the organisations for the opportunity to carry out a comprehensive risk assessment based on the OCTAVE Allegro methodology, but our offer was turned down, due to the sensitivity of the work, and the resource commitment that was required to make it a success. Therefore, we are aware of the limitations of our assessment, since it fails to reflect the risks and priorities of the organisations as required in the study of (Butler & Fischbeck, 2002).

A risk is estimated by the likelihood of an incident scenario, mapped against the estimated negative impact (ENISA, 2009). The level of risk will in many cases vary significantly with the type of cloud architecture being considered. One question we failed to ask in our risk assessment was if the CSP owned their hosting infrastructure, as it would have helped us in the estimation of the likelihood of a supply chain incidence. To assess the risk of each CSP to cloud supply chain failure, we adopted the qualitative risk assessment (RA) method since our questionnaire was written in a 5-point Likert scale format with seemingly non-numerical labels. The qualitative assessment is often argued to be a subjective method, but as Jeff Lowder (2008) points out, qualitative RA is compatible with objective and non-objective estimates of probability. Qualitative RA uses intervals to represent both the probability and impact of an outcome using an interval scale, where each interval includes a range of numerical value (Jeff Lowder, 2008). For each organisation, we rated their risk to supply chain disruption as low, medium or high. We applied a risk scale mapping which is similar to that of ENISA (2009), and it is as shown below:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk: 6-8

In the course of the study and after the analysis of participants' response to the Payworq case study, we had gathered some transparency features that could be useful in comparing cloud providers on the information they published on their websites. We examined twenty-five SaaS vendors, which were conveniently sampled from a list of the top 200 UK public cloud computing providers identified by Cloudscape (Bilderbeek, 2014). The company behind cloudscape, METISfiles, is a market research & consulting firm dedicated to solving strategic issues for executives in the digital economy and digital infrastructure industry (Bilderbeek, 2014). METISfiles also publish similar reports for cloud providers in Belgium, Denmark, Finland, Germany, Netherlands, Norway, Spain, and Sweden. We opted for the UK version of the Cloudscape report because it is local to the research team, and also provided us with the best chance of following up with the identified cloud providers in our future

research work. We thoroughly examined each vendor based on the information published on their website detailing our defined transparency features. Cloudscape categorised SaaS providers under seven main headings including an eight catchall category, "other". Out of the seven main categories, we compared SaaS providers in five different cloud service category namely: online workspace, finance/ERP, human resource management (HRM), customer relationship management (CRM), and collaboration (Bilderbeek, 2014). Similar reports to cloudscape also exist, but they were deemed unsuitable for this research. The organisations behind other considered reports include Microscope, Eurocloud, Montclare and Cloud directory.

Lastly to verify our work on the comparison of CSP transparency based on the information on their websites, we asked a cohort of fifty MBA students who were taking a supply chain elective module at the Said Business School (SBS) on their thoughts on cloud supply chain transparency. We gave them a list of six randomly selected cloud providers, which were different from the ones we earlier analysed and asked each respondent to investigate the supply chain of one of the CSPs, using their date of birth, to randomise their choice of CSP. A non-technical questionnaire was developed (see Annexe B) with the aim of assessing the participants' opinions on the transparency of their chose CSP. They were also required to help identify what will be their top reason for demanding transparency from a company that utilises third party sub-providers and if they were happy to use their chosen cloud service based on the information available to them on the provider website. This exercise gave us the opportunity to assess how business leaders and non-technical consumers perceive the transparency issues in cloud computing and verify if transparency of supply chain is a potential limiting factor to cloud adoption and the increase in cloud usage. Although we recognise that these graduate students might not all have the appropriate business experience or an established decision-making strategy, and might have a different attitude to risk-taking, but considering the early stages of this research, we wanted to establish a baseline for future work. We believe that the decision-making on cloud supply chain is one that is similar to production scheduling, which the research of Remus (1986) proved that MBA students with little business experience can safely be used as surrogates for managers.

The University of Oxford ethical approval committee, under Ref No: R44459/RE001 approved this research work involving external participants. The research plan described the use of the qualitative method of research (interviews, case studies) and the recruitment of participants to take part of the survey. Other details around the anonymity of participants' data and seeking permission from interview respondents to be recorded was requested and approved by the board. All data collected during this research. All participants were presented with a consent form detailing the purpose of the study, its ethics committee approval and their ability to withdraw their data at any time. We also assured the participants that their data would be stored securely following the University of Oxford ethical standards.

## **4. Results and Discussion**

### **4.1 Introduction**

In this chapter, we discuss the results obtained from our case study, interview, risk

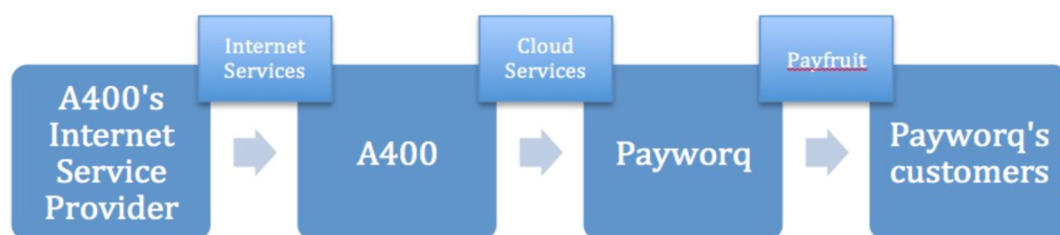
assessment and cloud provider website comparison. The participants for each of the methods used in this research volunteered themselves to participate. We utilised different recruitment strategies for each stage of the research. For the case study and risk assessment, some of the respondents were sent emails with a link to the google form used for the case study and RA, while we approached the other participants directly. The participants for the interview volunteered themselves to take part in the research, and most of those interviewed were vendors at the Cloud Expo in London. The individual research activities are discussed in the following sections with emphasis on our research questions. After which, we summarise the chapter with the findings of our work.

## 4.2 Case study

*Payworq Ltd offers payroll-processing software (PayFruit), which runs as Software as a Service (SaaS). Its move to the cloud was due to an increased demand for PayFruit, from small businesses and start-ups. Payworq needed an Infrastructure-as-a-Service (IaaS) provider to host its growing service, and it looked for the cloud service providers (CSP) from provider websites and attending exhibitions and trade events. Eventually, it selected A400 Ltd on its promise of flexibility, rapid scalability, redundancy, pay-as-you-use, and compliance with standards. Leveraging A400's expertise for hosting infrastructure services, Payworq could now focus on its core competency, which is software development.*

*Recently, PayFruit suffered a downtime for approximately four hours as a result of a power outage at the A400's Internet Service Provider (ISP). The situation was very damaging for Payworq; several of its customers were unable to pay their staff on time, and it now faces financial penalties.*

*As part of its incident management process, Payworq has arranged a meeting with A400 to try to ensure that this incident doesn't happen again. It wants to know more about the 'supply chain' of other providers, which may lie behind A400's offering. They want to follow this up with a comprehensive risk assessment of the benefits and vulnerabilities of their cloud solution.*



**Figure 2:** Payfruit cloud services supply chain.

We sent the above case study to a total of 47 contacts, which were made up of SaaS and IT industry experts, but only 12 of them responded, all of who were male, giving us a response rate of 25.5% over the three month period. The twelve responses received were of good standard, judging from the level of analysis of the case study that was carried out by each of the respondents. The two questions that accompanied

the case study connect back to our research objective of finding out the effect of transparency in reducing the supply chain risks in cloud computing. The questions are as follows:

- *What information should Payworq ask for? Cloud computing services are often sold on the idea that customers don't need to know the exact detail of the operations of their Cloud Service Provider's operations: but is this a good idea?*
- *How much should A400 be prepared to tell? Providers are often reluctant to reveal too much about their operations - even to customers. What are the issues about being completely transparent about your operations?*

Before we analyse the response of our participants, it is important to lay the foundation as to what makes this case study particularly interesting. In the course of this research, we have identified that cloud services are usually delivered with one or more levels of abstraction. Also, we highlighted how according to CSA, due diligence is a top risk in cloud computing. Raj Samani (2011) also supports this view, saying, "if you cannot be sure how your data will be treated, and that it will be adequately protected, then it would be reckless to go blindly into the cloud, even if the economic benefits look attractive". Furthermore, evidence shows that SMBs engage in a near-term strategy to reduce cost and increase productivity, and IT services, including cloud computing, have been identified as a crucial area with a large margin for improvement (ENISA, 2009). From the case study, we see that the downtime suffered by Payworq prompted them to enquire more about A400 Ltd.'s supply chain. It seems Payworq was not aware of the CSP sourcing its Internet access from a single ISP and might have selected A400 without proper due diligence. We would now turn our attention to the responses of our participants.

### **Research Question 1: What information should cloud customers ask CSP about its supply chain?**

In practice, the information a customer can ask CSPs outside the information readily available to them from provider websites, and marketing document cannot be easily estimated. Large customers are known to be able to get CSPs to respond to their request for information (RFI), because of their higher purchasing power. However, the same cannot be said of SMBs, who according to Raj Samani (2011) get little cooperation, let alone answers when they submit questionnaires to large corporations. Interestingly, according to a World Bank research, SMBs accounts for 95% of existing businesses and their products and services make-up around 49.8% of the global economy (BCSG, 2015). Therefore, it is important to know what sort of information CSPs should always be willing to provide irrespective of the size of the customer, especially when the client explicitly requests for the information.

The response from our participants elicited a range of ideas. Over half of the replies contained the need for the cloud customer to have a high-level understanding of the architecture of the CSP's infrastructure. One of the participants commented: *"The underlying infrastructure provider should not be a secret, and CSP should be willing to share high-level details of their architecture and dependencies on 3rd party providers even if the exact nature of their product code remains confidential"*. Zhang et al. (2010) established a correlation between the security risk associated with a cloud delivery and its cloud architectures and security controls. It is a widely known

fact that nested cloud architectures further exacerbates the threats and vulnerabilities of implementations such as cloud federation, and keeping this information away from the customers makes it difficult for them to assess and ultimately mitigate such risks. Some other responses to the question, concerning the architecture, *requested that the customers should seek details of high availability within each of the CSPs datacenter. Also, there was a call for the request of the escalation process; confirm how outage is detected and handled; request details of any other existing single point of failure and verify what has been done to prevent a repeat of the disruption.*

Another interesting aspect of our respondent's feedback was the definition of service level agreement (SLA). Eight of the respondents requested the CSP to provide further details on their SLA with regards to the outage, and one participant asked to know if there was going to be compensation. Some of the other comments on SLA include: *"ask for figures on reliability and availability, as those are indicators of the professional level of operations"* and *re-confirm your compute and storage SLA*. One respondent suggested Payworq to *"get an understanding of the CSPs uptime record as well as SLA, as this helps Payworq in setting their own SLA to their customers"*. Conversely, one of the respondents was quick to add the following: *"from a contractual perspective, Payworq should ensure they understand the SLA, 4hours represents 0.5% (roughly over a month), so if they have a 99.5% SLA, then the outage is still within SLA tolerance"*. As seen in the case study, it is assumed that an SLA was already agreed between Payworq and A400; however, the incidence at A400's ISP was the cause of the outage of the PayFruit service and possibly other customers of A400. Such occurrence is an example of the reliability and performance issues that poses a unique challenge with cloud computing as contained in the COSO Enterprise Risk Management Guide (Chan et al., 2012). One could argue that had Payworq known about their CSP's dependence on a single Internet provider, and Payworq might either have chosen a different vendor or implemented a standby system to mitigate this sort of outage. A respondent went further to say that *"SLAs should go beyond highlighting availability, uptime, DR and BCP terms and should include security controls and how the CSP plans on implementing them"*.

Some of the other information highlighted by the respondents are listed as follows

- i. **Monitoring and Notification capabilities:** *Ask for proof on how well the CSP monitors their infrastructure and enquire about the parts of their operation that is dependent on third parties. How do they identify what nodes/data have potentially been compromised?* One respondent mentioned that: *"CSPs should concentrate on procedures for notifying clients of problems rather than detailed internal operations"*.
- ii. **Certification and Audits:** *Customers should ask CSPs for the professional and third-party certification of their operations. Also, request independently verified audit reports such as the Service Organization Control (SOC) 1 and SOC 2 Type II reports.* The SOC 2 Type II reports on the providers controls relating to security, availability, processing integrity, confidentiality, and privacy of a system (SSAE, 2016). The SOC 2 report also gives visibility to the supporting services provided by sub-service providers, which may not be known to the customer.

- iii. **Security Controls:** In addition to the high-level architecture, the case study participants believe customers need to know about security controls implemented by the CSP to protect their data. These controls include physical security, network security and application security. This request also chimes with the research of the Cloud Council in their guidance document - Security for Cloud Computing. In the guidelines, they suggest that cloud customers should prove enforcement of provider security controls by requesting appropriate access to providers events, logs and audit trails (Council, 2015).

## **Research Question 2: How much should CSP be willing to share with their customers?**

Hofstede (2002), in his paper titled transparency in netchains, asked this question: "If the entire netchain is transparent, who benefits? He considered all the actors that need additional information, including the role of government, together with the cost and workload involved in achieving transparency. He also added that it can be a strategic decision not to be transparent. He defined transparency of a chain as the extent to which all stakeholders in the chain have a shared understanding of, and access to, the product-related information that they request, without loss, noise, delay and distortion (Hofstede, 2002). This definition, if applied to cloud computing seem to suggest that cloud customers, should have an understanding of and access to information on the supply chain of their cloud service. Although, we also know from our literature review that Hofstede (2002) argues that supply chain information should not be provided unless requested because knowing what information the customer wants is a precondition for transparency. Earlier, we established that the cloud supply chain could be fluid and dynamic with no permanent partners or customers. Therefore, knowing that there is a genuine risk of industrial espionage, sabotage, malicious attack, or even reputational damage as a result of supply chain visibility, how much information should CSP be willing to share with their customers?

We address RQ2 in the second question of the case study we put to the respondents. All 12 participants answered the question in depth, and a few of the responses seem to give us insight to how the respondents implement transparency within their organisations. Without repeating the details of what customers should ask from their CSP, which nine of the respondents agreed CSP should be willing to share, we present some of the responses that shed more light to the second research question.

One of the participants encouraged information to be shared *as long as it didn't break the intellectual property of the CSP*, a suggestion similar to that of Chopra & Sodhi (2004), in their article managing risks to avoid supply-chain breakdown. Another respondent suggested that *the CSP should be prepared to tell as much as the customer will understand*, which we felt was promoting information asymmetry and could be advantageous to larger organisations with more technical resources, and less so for SMBs. Nevertheless, this respondent's view is in line with that of Akkermans (2004), who says data transparency alone is not enough, but the data needs to be understood by the recipient. Another respondent referenced the notion of providing customers sufficient information to assess their risk, stating that: *"the exact topography and schematics do not need to be shared, but A400 should be prepared to discuss where their solution has a reliance on a 3rd party e.g. Rackspace, etc."*

In analysing the other responses received, we identified that about three of the respondents were against full disclosure of the CSPs supply chain, with one respondent asking *why A400 should provide details of their supply chain when most businesses do not*. Although the participant's response seems to be biased, because he follows this with making a pitch for his organisation's vendor-agnostic monitoring tool. Similarly, another respondent against CSP disclosing their supply chain to their customers claims *it is an issue of confidentiality. He notes that since there are lots of customers sharing the platform, little information is in order, as less information is more security (i.e. security by obscurity)*. The respondent argues that customers should deal with their direct provider, and worry less about the supply chain of the cloud service. However, the security community, especially renowned security commentator, Bruce Schneier, has frowned against achieving security by obscurity. Schneier says in one of his publication that, if algorithm must remain secret for the system to be secure, then the system is less secure (Bruce Schneier, 2002).

Another perspective of supply chain transparency paradigm is that of trust. One of our participants in relating trust to the case study *believes that A400 needs to give Payworq enough information to build or retain trust otherwise they risk losing customers after such incident*. He went further to say that coupled with providing customers with high-level architecture, redundancy and security control information, CSPs can also share with their clients their process for choosing a supplier. All of this he claims gives the customer confidence in their cloud solution. Furthermore, in one of our participant's cynical comment is the issue of provenance cost. He says that *the cost of providing such information will be too great for the cloud provider, suggesting that people want the best, but are not always willing to pay for it*. Conversely, another respondent believes *"there shouldn't be issues with CSP being transparent with their supply chain information if they are offering an excellent service and are honest about their SLA, but stresses that customers need to understand that the last 1% of an SLA is the most expensive"*.

In summary, the case study gave us a good foundation in this exploratory research into the effect of transparency in reducing supply chain risks in cloud computing. We have been able to provide answers to two of our research questions, although we will continue to build on them in the subsequent sections. The participants' feedback on the information customers should be willing to ask their CSP provided us with some transparency features (security controls, architecture, SLA, DR/BCP, IT certification, technology partners), which we used in comparing CSPs on their supply chain transparency in the latter part of the study. Despite the limited number of participants, we feel the information gathered provides a good groundwork for future research on this topic.

### 4.3 Interviews

In this section, we discuss the findings of our data collected through in-depth semi-structured interviews with the cloud vendors. A total of 15 informal interviews were organised around a set of predetermined open-ended questions, with other issues emerging from the response provided by the interviewee. There was a free flow of conversation between both parties, which helped us to establish in a social context,

what cloud supply chain transparency meant to each participant.

At the start of each interview, we asked our interviewees how much they knew about their supply chain? As expected, some of the providers who hosted their infrastructure, were quick to say they were their own supplier, but with a little more clarity on the definition of a supply chain, as defined by Wisner et al. (2008), we were able to correct this notion. However, the responses were mixed, with the larger organisations knowing more about their provider's, up to about the second tier or third tier in rare cases, and the smaller SaaS vendors not quite so. One of those interviewed was the CEO of an original equipment manufacturer (OEM) for a private cloud infrastructure, and in our conversation, we gathered that although the product was assembled in the UK, the components were sourced from a major supplier in China. When asked, if there was a contingency in place, the answer was affirmative, but he admitted that since *they lack the visibility into the 2nd, 3rd and 4th tier suppliers, there is no guarantee that both major supplier's arrangement aren't dependent on similar sub-suppliers*. Furthermore, we gathered from some of the start-up firms that traceability most times comes at a premium, which they were not willing to pay. One interviewee sighted a few examples of companies which started as a small start-up and later progressed into large firms, saying companies only start to care about the risks of the supply chain as their customer base increases, or when reliability or security issues can lead to a reputational loss. He added that *".... Dropbox, when they initially hosted their service on AWS, wouldn't have cared about AWS supply chain, as long as they got a cheap and reliable service. But the story has now changed since they now store customer data using in-house datacenters"*. It seems the cost narrative is a common one even amongst end-users, who are willing to use a cloud service for free, disregarding its terms and condition, including claims to use their data for marketing purposes.

When asked why some CSP did not prioritise supply chain risks or the general risks of cloud computing, the interviewees pointed out that although they thought about it, it is hard to assess a worst-case scenario. One respondent added that: *".... the fact that no major event resulting in multi-billion dollar loss has happened in the cloud doesn't mean one won't occur shortly, but we don't know any better"*. Which brings up an interesting observation by New & Brown (2012) concerning how the Japanese earthquake of 2011 changed the perspective of manufacturing organisations to supply chain risks. Perhaps, it will take a significant breach or downtime to one or several cloud giants before the cloud community can be awakened to the realisation of the complex commercial interdependencies that exist in cloud computing and its resultant risks, a point also echoed by Pearson et al. (2012). Some of our interviews led to the conversation on cloud insurance, which from what we gathered is beginning to take shape in the cloud computing industry. In 2013, MSPAlliance in partnership with Lockton Affinity, a large privately owned independent insurance broker, announced a new Cloud and Managed Services Insurance (Reuven Cohen, 2013). The uncertainty of the effect of cloud risks has led providers who retain liability as part of their customer contracts to reduce such liability by taking up an insurance contract (Weber & Staiger, 2014). Although outages are part of today's technology landscape, many cloud providers have built their reputation on the resilience of their service, and as such have attracted more risk adverse customers and are therefore in need of extra assurance or comprehensive protection (Reuven Cohen, 2013). Weber & Staiger

(2014) further categorises the potential cloud risks subject to the insurance as, data, privacy and regulatory risks, security, service failures, loss of operational control and supplier risk. These risks could have their insurance cost broken down into first party (direct) and third party (indirect) costs. The first party risks are the risks to the CSP, which are hard to calculate but can be fixed through liquidated damages provisions, while the greater risks lie in claims made by third parties e.g. when a customer claims for loss of access or destruction of data (Weber & Staiger, 2014).

An academic consultant working with one of the SaaS providers we interviewed, summed up the issues he sees with cloud computing using three ideas and they are as follows:

- *We must trust our CSP before we hand our data over to them.*
- *We don't know what is going on in the cloud.*
- *Not sure what happens, if our data gets lost in the cloud.*

The issue of trust as earlier discussed in the literature review is one that is essential for cloud survival. Das & Teng (2001) were able to establish the linkage of trust and control with risk when dealing with strategic alliances. Cloud provider relationship with a customer is a strategic one, especially when the cloud service offers an innovative technology, which the client leveraged for competitive advantage. Although, one of our interviewees pointed out that the situation of transparency and trust is a catch-22, saying, *"If I tell you, you might know my weakness. If I don't say, you do not trust me."* According to Akkermans et al. (2004), there is a feedback loop, whereby the increase in trust leads to increase in transparency, which improves decision-making quality and improves supply chain performance. One of the respondents sighted the example of how his organisation adopted the "travail" method of transparency, suggested by Akkermans et al. (2004) to help their customers understand how much effort goes into securing their data. The CSP, who host their service in AWS, told us *how they take prospective or current customers on an arranged tour of an AWS facility, stressing that the rigour of the security checks they go through, gives the customers an assurance of physical security and that this improves the client's trust in their service.*

Backup as a Service (BaaS) is becoming a prominent "as a Service" connotation for storage in the cloud. After all, that is the service provided by traditional cloud organisations like dropbox, box, google and so on. In our interviews, we had the opportunity to speak with representatives of three cloud backup and storage solution companies, and their opinion on supply chain transparency is worthy of mention. We had earlier observed during our search on cloud provider websites, that the cloud storage providers were rarely referenced by CSPs that used their services. The reason provided by one of the respondents that was unknown to us at the time is that *"Whoever stores the data, owns the customer"*, an idea Luke Behnke, VP products at Bitcasa says is a *"key revenue-driving idea that has largely slipped under the radar"*. The interviewee added that in cases *where their SLA with the CSP covered loss or damage to data, the liability was theirs*, which many a time is not known to the customer. Another respondent went further to tell us the reason for the blur in supplier details. In his words, he says, *"The legal framework of storage and compute outsourcing depends on the commercials. Companies engage with a storage vendor, and as part of the agreement could decide to keep the relationship of supplier secret."*

Some of the organisations we spoke to now have smart solutions using REST API to accompany data into the cloud, hereby giving the customer control and visibility of their data, irrespective of the CSP controls.

Furthermore, by coincidence, we came across a classification of Chief Technology Officers (CTOs) and their preference for visibility of controls in the cloud. We later tested this notion with all other participants we interviewed and found it to be relatively correct. We learnt CTOs could be categorised into the millennial vs. "old guy". The analogy is that millennial CTO, who grew up in the social media age, who has information at his fingertip and who demands innovation in technology, is less apprehensive about cloud computing risks, data storage location or security controls implemented in the cloud. Whereas, the "Old guy" CTO, who started working in the days of the mainframe computers, who is used to having his datacenter under lock and keys, and who loves the look and feel of the rack of physical kits in his DC is much more apprehensive. The older CTO seems to feel less in charge of their data, and this is something they are not used to, and might take a while before they adjust. It was agreed amongst the interviewees that CTOs who are hands-on, want to know the location of their data and the efforts CSPs take to protect it.

In conclusion, we found out that the transparency of supply chain is a customer-driven process. Many of the CSPs confirmed that most customers do not ask for too much information about the cloud service or its supply chain but are more concerned with the cost. Also, we learnt that the reason many customers used AWS or Rackspace instead of the smaller public cloud providers was that, they paid less attention to where their data was stored or who had access to it, as long as the service was cheap. For the CSP, there is an incentive to establish trust with their customers, and this can happen when they can provide the needed information to them. The advice is for CSPs to start simple and get comprehensive if needed. Cloud providers who automatically update their service status, uptime and SLA targets on their web portal for their customers to see, are also challenging themselves to optimal performance. We identified the reason for the blur of vendor information sometimes for competitiveness and exclusivity, but also recognise that the transparency of cloud suppliers can also be leveraged for trust, as was the case with some of the start-ups we interviewed who branded their solution with Amazon AWS. Except for two interviewees, all others were in support of more transparency from the cloud providers, both through their online presence and in their day-to-day relation with their customers. Although this could cause a particular bias, considering they might consciously or unconsciously want their organisation to look good from the outside, more so as it related to security. Our opinion as a whole is that the interviewees were genuine in their views, and they were forward thinkers, who looked to make cloud computing secure for customers.

## 4.4 Risk Assessment

In assessing the risk of a cloud computing environment, there is a challenge of choosing the right risk management framework that will help uncover key risks, prioritise those risks and develop a mitigation plan. According to Gadia (2011), the options available to Information System auditors include generic frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO)

ERM; or IT domain-specific risk frameworks, such as ISO 27001 and ITIL. There is also bottom-up guidance to cloud computing that exists from bodies such as CSA, ENISA, and NIST. From the evidence currently available, it seems fair to suggest that of all the risk frameworks, the ISO 27001 is the most widely accepted risk management framework among CSPs, possibly because of its domain-specific guidance. However, an analysis of current risk controls for cloud computing conducted by Auty et al. (2010) found the ISO27001/27002 controls to be unsuitable for cloud computing. They identified fourteen possible aspects where the ISO standard was unable to address cloud-associated vulnerabilities.

As noted in the methodology, our risk assessment questionnaire, which is specifically addressing supply chain risks, was drawn from COBIT, CSA CAIQ and the research of (Kleindorfer & Saad, 2010). The COBIT framework helps to fill the gap between generic risk management frameworks, and domain-specific frameworks, while the CAIQ is a bottom-up guidance from CSA, which is unique to cloud computing. At the end of our study period, of the 45 people we approached directly or contacted through email, 12 respondents completed the questionnaire. The respondents were all cloud providers in the UK and the breakdown according to cloud service is as follows: 5 SaaS providers, 5 PaaS providers and 2 IaaS providers. The response rate was 26.6 % over the 3-month period of April and June 2016. The respondents were also asked to indicate the size of the enterprise, which yielded an even result across the small, medium and large organisations.

In this section, we carry out the analysis of our participants' response to the questionnaire, followed by the qualitative risk assessment of each participant to supply chain failure.

The first question in the questionnaire, was aimed at establishing if the organisations had an organisational ERM and whether business risk assessments included cloud-related risks and the response was as follows:

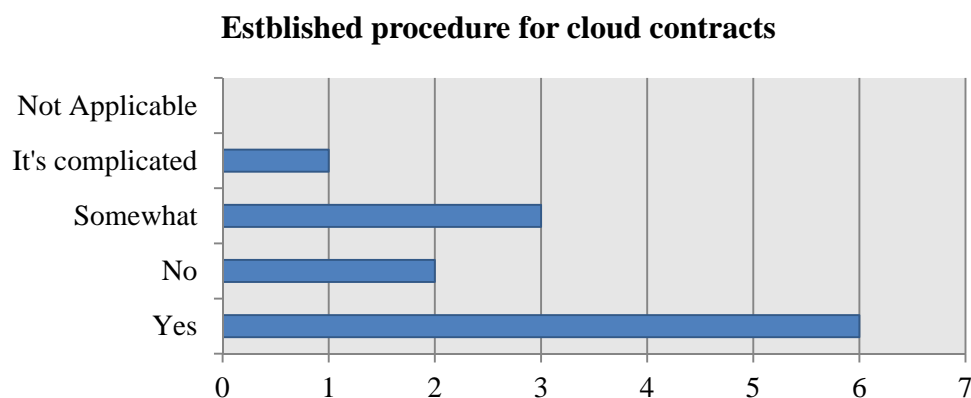
- Eight respondents answered, "Yes."
- Two respondents answered "somewhat."
- Two respondent answered "No."

Although with a small sample size, caution must be applied, as these figures are not a representative of the wider cloud provider community. However, the result shows that organisations that have an ERM governing their business processes, still fail to include cloud risks in it, despite the potential damage a cloud risk could have at the firm. Chan et al. (2012) suggest that there could be a damaging effect if management neglect to perform the time-consuming tasks such as evaluating the potential impact of the CSP on the organisations operations and risk profile.

According to Marston et al. (2011), one of the ways an organisation can understand and prioritise its supply chain risks, is for them to stress-test their infrastructures. They see it as an effective way of gaining buy-in and shared ownership within the chain and across project teams. Chopra & Sodhi (2004) says that stress testing should be positioned as a "thought experiment" that can help the companies to prepare for unforeseen events as well as identify key suppliers, customers, etc. We asked respondents *"if their cloud infrastructure goes through stress testing at least once a year to consider internal and external risks"* and 7 of the 12 respondents carried out

stress testing, and two answered, “not applicable”. In analysing the questionnaire of the two respondents who answered “not applicable”, we suggest that this might be because they believe their multiple supplier solutions in one case, or the horizontal scaling of their system across multiple Amazon regions in the case of the other, is enough to protect them from disruptions. In our opinion, solutions of this nature are heavily provider-dependent, and the organisations failed to realise that not all risks can be mitigated by contractual clause with a CSP as opined by Chan et al. (2012).

On the subject of contracts, we asked the respondents if they “*have an established procedure for setting up, modifying and terminating supplier contracts*”, and the result is as shown in the bar chart below.



**Figure 3:** CSPs that have an established procedure for contracts

In this assessment, we took the “it’s complicated” answer as the respondent is not aware of the existence of such process within their organisation or that the process is not properly established. The more an organisation uses a provider’s solution in the support of its operations, the more it depends on the CSP (Chan et al., 2012). This dependence can develop into a vendor lock-in situation, where the customer is unable to leave the CSP or the cost of moving becomes prohibitive. Every organisation with services in the cloud, need to develop an entry and exit strategy or contingency plan as part of their overall cloud strategy (Chan et al., 2012).

As discussed earlier, the CAIQ, which is functions as a cloud supply chain’s risk management and due diligence questionnaire, provides CSPs with an opportunity to demonstrate compliance with the CSA cloud control matrix (CCM) (Pohlman, 2010). With the responses we received from the respondents, we can see a distinct lack of reporting by CSPs to their customers. In the best case scenario, where an organisation carried out a risk assessment to select the CSP that fits their risk profile, such assessment is only accurate on the day of evaluation, similar to a “car’s MOT test”. With the evolving nature of cloud risks, which calls for an evolution in cloud risk management, customers are in a bad position if they do not receive regular reports from their CSPs. When we asked the respondents if they “*receive regular reports from our third party suppliers outlining compliance and adherence to all policies (internal, external, regulatory or contractual)*”, only five answered “yes”, and five answered “no”, with the other two responding as “somewhat”. The failure of a CSP to renew a compliance accreditation negatively affects the customer, and such

information needs to be made readily available to customers without the need to request for it.

There were better results with CSPs (SaaS/PaaS) being aware of the software or hardware operated by their cloud providers. We believe this is because technically there are peculiar features of hardware and software, which experts familiar with those systems can extract, to identify the underlying platform. Also, all our respondents were confident, and they answered “yes” when asked if they were aware of the *transmission of their sensitive data being done over a trusted path with controls in place to provide confidentiality, authenticity, non-repudiation, etc.* The result goes to show that the CSP and potentially their providers are at least providing secure communication that can be verified. Furthermore, all our respondents except one had *controls in place to mitigate and contain data security risks within their supply chain.* Bhensook & Senivongse (2012) in their assessment of compliance of CSPs to security requirements, identified consumers concern over data security as one of the key barriers to the adoption of cloud services. We suggest that it is not enough for cloud providers to have controls in place to mitigate data security risks; they should disclose sufficient information about these process, practices and procedures to their customers, for the customers to build trust in them.

In Kleindorfer & Saad (2010) research into managing disruption risk in a supply chain, they argued that risk avoidance should precede risk reduction, based on the understanding that any investment in risk assessment should look to determine key vulnerabilities, as well as the worst-case scenario that can result from such vulnerability. Following this initial step, organisations can work on contingency plans and prioritise mitigation plans. We put the question to confirm this approach to the respondents: *Our risk assessment model favours risk avoidance over risk reduction*, and of the 11 respondents that answered the question, only two favoured reductions over avoidance, while all others agreed with Kleindorfer & Saad (2010). A possible explanation for the respondent who didn’t answer the question is that he/she didn’t understand the question enough to provide a reply, considering that was the only question left unanswered. As for the two respondents who favoured risk reduction over avoidance, we suggest that, perhaps, their organisation's risk appetite, as well as their cloud solution, supports such decision.

Also, we gave each of the respondents an opportunity to tell us more about the way they handle cloud supply chain risks, and only 5 of them provided feedback. Two of the feedbacks were not answering the question, but providing us more information into the reason for some of their answers e.g. the provider we mentioned, who horizontally scaled their cloud solution across multiple Amazon regions. The comments provided by the three respondents are as follows:

“ *We make use of multiple suppliers for our cloud service.*”

“ *We make a list of our identified cloud risks and monitor them, while working on reducing them to an acceptable level.*”

“ *We have established a continuous audit program with our suppliers.*”

Lastly, we carried out a risk analysis for each of the CSP, who filled the questionnaire and the result is as shown in the table below. These results are somewhat consistent

with that of ENISA (2009), who although did not carry out a comprehensive risk assessment, based their estimation on a realistic use-case scenario and considered a total of 23 risks including supply chain failure. The majority of the cloud providers had a low probability of a supply chain failure, which we put down to the resilience built into cloud architectures in general. CSP "A" had such a high risk of supply chain failure because they were not as aware of their supply chain in comparison to others. Also, they did not demonstrate their ability to mitigate risks outside the control of their CSP. It is possible, therefore, that being a start-up firm, they are focusing on their core competency and hoping their CSP can do a good enough job to keep them productive. As for CSP "L" and "E", which both had the least risk score, their response to the questionnaire would seem to suggest that both organisations have thoroughly considered the risks of their supply chain, and have processes in place to avoid disruptions in their cloud service. Additionally, it is important to bear in mind the possible bias in the response of the participants to the questionnaire, perhaps to make their organisation look good and boost its reputation. We, however, reminded them of the anonymity of this report, so we do not see the reason for them to falsify their answers.

Cloud Service Provider (CSP)	Cloud service Model	Size of organisation (No of Employees)	Probability	Impact	Risk of supply chain failure	Risk Score (0-8)
CSP A	SaaS	1-9	Medium	High	High	6
CSP B	SaaS	Over 250	Low	Medium	Medium	3
CSP C	PaaS	10-50	Low	Medium	Medium	4
CSP D	PaaS	Over 250	Low	Medium	Medium	4
CSP E	SaaS	Over 250	Low	Low	Low	1
CSP F	SaaS	1-9	Low	Medium	Medium	3
CSP G	PaaS	Over 250	Low	Low	Low	2
CSP H	SaaS	50-250	Low	Medium	Medium	3
CSP I	PaaS	10-50	Low	Medium	Medium	4
CSP J	IaaS	1-9	Low	Medium	Medium	4
CSP K	IaaS	50-250	Low	Medium	Medium	3
CSP L	PaaS	10-50	Low	Low	Low	1

**Table 1:** Risk assessment of cloud providers

Overall, we see that the transparency issue between cloud providers and consumers is one that has its root in the cloud supply chain. We hypothesise, that in some cases, the non-provision of supply chain information between CSP and customer, is not down to the non-transparency of the CSP, but for lack of information. Hence, a CSP, who outsources a critical part of their cloud service to a third party, can experience disruptions to that service due to one weak partner in the supply chain, unknown to them.

## 4.5 Cloud provider comparison

The growing trend in cloud adoption has seen a surge in the number of companies rolling out public cloud services, to meet their customers need. The many success stories of SaaS applications have demonstrated the relative ease at which start-up companies can launch a cloud service, with no upfront cost, and within few months

boast of a sizeable customer base. In the support of diverse customers needs, the purpose of these cloud applications can range from BAU to strategic goals. From CRM to HR applications, there is an endless list of cloud providers, which also fosters healthy competition amongst the CSPs. However, the variety of cloud providers makes it more difficult for a cloud customer to choose which CSP best fits their requirement. Listing 50 SaaS vendors, who specialise in cloud desktop service, has become relatively easy, but finding the best provider based on security, performance, availability, etc. has become more difficult. According to Li et al. (2011), the reason for this is because there is no detailed, comprehensive comparison between the CSPs since the majority of the CSP publish a vague specification of their cloud offering. Many customers end up signing up for a cloud service, only to find out that their SLA cannot be met, or the cloud company is managed out of their provider's home office. Therefore, our focus was to compare SaaS providers, whose services could potentially be bought online, by a new customer looking to adopt cloud services and who based his/her decision on the information available on CSPs website.

In the previous sections, we looked at the effect of supply chain risk management in the adoption of cloud services. With the variety of cloud providers and the limited available information to comprehensively compare them, we decided to carry out a comparison of cloud providers based on some transparency features we identified from our case study exercise and some literature reviews. Talluri et al. (2006) discussed how traditionally, vendor evaluations have been based on financial measures with less emphasis on other tangible or intangible criteria but how this trend has changed, leading to the use of methodological developments in vendor evaluation techniques. The methodological approach base vendor evaluation on the consideration of multiple measures that often included product and service-related attributes (Talluri et al. 2006). We applied this methodological approach in our comparison of CSPs and centred our comparison on eight transparency features, namely:

- Architecture
- Technology/Partners
- Datacenter location
- Security features
- IT-related compliance certifications
- Advertised Service Level Agreement (SLA)
- Disaster recovery/ business continuity
- Monitoring/Support

In the psychology of security, Schneier (2008) asserts that “Security is both a feeling and a reality; and they are not the same”. We argue that it is not “OK” for CSPs to ask their customers to trust them with keeping their data secure, without the cloud solution appealing to the feelings of the clients and addressing the potential security risks in a manner that customers will feel safe and secure (Demsash, 2012). Therefore, we approached each of our CSPs website with the goal of finding any published information on the above transparency features. As each CSP is unique in their cloud offering, so also are their websites. To stay fair in our analysis, we had to search each CSPs website thoroughly, ensuring that all information relevant to our transparency features were considered. The following table describes the criteria against which each transparency condition was measured during the analysis of CSP's website.

#	Transparency Feature	Description
1.	Architecture	Under Architecture, our aim is to find details of the high-level architecture of the CSPs cloud offering. We look out for technical specifications of the network, security, storage and server infrastructures that deliver the cloud service. For example, a SaaS provider could mention how their server infrastructure is protected from malicious traffic and the high availability functionality of their cloud solution.
2.	Technology/Partners	Here, we are looking to see if SaaS providers mention their IaaS hosting provider and in the case where they own their infrastructure, their hardware, software and internet service providers. For example, Capsule CRM publish that their servers are hosted in Amazon's data centres while Fifosys a SaaS and IaaS provider, also have companies like Cisco, Citrix, Equinix and Microsoft as their partners.
3.	Datacenter location	The choice of datacenter location as one of the criteria is to help customers in determining the jurisdiction under which their data is stored. A cloud vendor, that hosts their service within the UK, gives the customer the assurance that they will be protected under the EU data protection directive.
4.	Security features	Here we look out for the mention of security controls implemented by the CSP to protect their cloud service. Features that include encryption, (physical, server and application) security, high-availability, password protection, etc.
5.	IT-related compliance certification	With IT certification, we look for SaaS providers, whose organisation has gone beyond leveraging their providers' accreditation, to obtain theirs. Certification like ISO27001, Payment Card Industry (PCI) and cyber essentials are common amongst these providers.
6.	Advertised SLA	With SLA, we look out for CSPs that have explicitly provided details on the availability of their product and how quickly they expect to respond in the event of an incidence. It is also useful for customers to know what the average uptime of the cloud service has been over the year, and if the provider has a track record of meeting SLA.
7.	Disaster Recovery/ Business Continuity	Here we look for CSPs that have mentioned data backup, RPO (Recover Point Objective) and RTO (Recovery Time Objective) on their website. We also considered where CSP provided details of their failover datacenter for resiliency.
8.	Monitoring/Support	With monitoring and support, our aim was to find details of the support helpline, and the mode of operation (e.g. 24/7). We looked out for alert and notification methods deployed by the CSP to provide their customers with service related information.

**Table 2:** Detailed description of CSP comparison criteria.

As we have discussed earlier in this study, trust in a cloud service can be enhanced based on the knowledge of the CSPs processes, architectures and visible controls, and this trust together with control reduces the perceived risk of a cloud service. Below is a tabular comparison of our 25 SaaS providers as conveniently sampled from the Cloudscape report (Bilderbeek, 2014).

SaaS cloud provider comparison based on Transparency features											
SaaS Cloud Provider	Architecture (Yes/No)	Technology/ Partners (Yes/No)	Datacenter location (Yes/No)	Security features (Yes/No)	IT-related compliance certifications (ISO 27001, PCI-DSS, ITIL etc.) (Yes/No)	Other cloud offering (PaaS, IaaS & Others)	Private, Public, & Hybrid	Advertised Service Level Agreement (SLA) (Yes/No)	Disaster Recovery/ Business Continuity (Yes/No)	Monitoring /Support (Yes/No)	Scoring (No. of Yes) Maximum=8
<b>Online workspace sub-group</b>											
Fifosys	Yes	Yes	Yes	Yes	Yes	IaaS and PaaS	All	No	Yes	Yes	7
Red centric	Yes	Yes	Yes	Yes	Yes	IaaS	All	Yes	Yes	Yes	8
Adapt	No	Yes	Yes	Yes	Yes	IaaS and others	All	No	Yes	Yes	6
Frontier technology	No	Yes	Yes	Yes	Yes	IaaS and others	All	Yes	Yes	Yes	7
NASSTAR	Yes	Yes	Yes	Yes	Yes	N/A	All	Yes	Yes	Yes	8
<b>Finance/ERP sub-group</b>											
Kashflow	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
Quickfile	No	No	No	Yes	No	N/A	public	No	No	No	1
Statpro	No	Yes	Yes	Yes	Yes	IaaS	All	No	Yes	Yes	6
Boox	No	No	No	No	No	N/A	public	No	No	No	0
Webexpenses	,	No	No	No	No	N/A	public	No	No	No	0
<b>Human Resources (HR) sub-group</b>											
BreatheHR	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
Clearbooks	No	Yes	No	Yes	No	N/A	public	Yes	No	Yes	4
Natural HR	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
Youmanage	Yes	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	7
Staffcare	No	No	No	No	No	N/A	public	No	No	No	0
<b>Customer Relationship Management (CRM) sub-group</b>											
Capsule	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
Intrabench	No	No	No	Yes	No	N/A	public	No	No	Yes	2
TrackerRMS	No	Yes	No	No	No	N/A	public	No	No	Yes	2
Workbooks.com	No	Yes	Yes	Yes	No	IaaS	public	Yes	Yes	Yes	6
Apiscrm	No	No	No	Yes	No	N/A	public	No	No	Yes	2
<b>Collaboration sub-group</b>											
Groupspaces	No	No	No	Yes	No	N/A	public	No	No	No	1
Huddle	Yes	Yes	Yes	Yes	Yes	N/A	public	Yes	Yes	Yes	8
Winweb	No	Yes	Yes	Yes	No	N/A	All	Yes	Yes	Yes	6
Skyscape cloud services	Yes	Yes	Yes	Yes	Yes	IaaS and PaaS	All	Yes	Yes	Yes	8
Kahootz	No	Yes	Yes	Yes	Yes	N/A	Public	Yes	Yes	Yes	7

**Table 3:** Comparison of 25 SaaS providers taken from Cloudscape

Table 3 shows the results obtained from the comparative analysis of the 25 SaaS providers. Although this comparison is far from authoritative, considering our method of gathering the data, we believe it is a good start and could be developed further to establish the minimum level of information CSPs should publish on their website; thus boosting cloud transparency. To avoid comparing cloud providers that target different industries, we categorised our 25 CSPs into five groups namely: online workspace, finance, HR, CRM and collaboration. Furthermore, we investigated various vendor evaluation techniques including simple weighted scoring methods, complex mathematical programming and neural network models (Talluri et al. 2006). In the end, we chose to go with a simple numerical scoring system, where for every transparency feature a CSP published on their website, we gave them one point and did not give any point for missing features, assuming each element is equally weighted.

From the data in Table 3, we can see that the CSPs in the finance/ERP sub-group scored the lowest points. One possible reason for this is the fact that the lowest scoring CSPs (web expenses, receipt-bank and quickfile) are vertical industry specific since they operate in the finance sector, where local knowledge and regulation is essential. Their websites only make reference to cloud hosting for a technological advantage, and all other contents are geared towards promoting how the software works, pricing and other marketing information. Surprisingly, with a mean score of 2.6, if we take these five companies as a representative of the finance SaaS providers, that would suggest that finance CSPs are not transparent with their cloud service. One would expect this not to be the case, considering that a company like web expenses, which helps accounts staff in small and large organisations with settling staff claims, will need to store personally identifiable information (PII) as part of the onboarding process. We argue that CSPs, who operate in financial or sensitive information industries, should provide as much information to their customers to improve their trust in the service and allay fears relating to loss of privacy.

In our analysis, CSPs in the online workspace sub-group were found to be the most transparent. With a mean score of 7.2, the five CSPs showed a clear understanding of their cloud architecture, provided detailed information about their cloud offering, and steps they took in securing customer data. We suggest that some of the reasons for this very positive result include the fact that at least four of the CSPs were also IaaS providers, who provided compute, storage, network capacity to other cloud providers (e.g. SaaS) as well as host their SaaS services. We believe that the organisations are technically adept in cloud technology and have made substantial investments in datacenters and other infrastructure, which they need to publish on their websites. We hypothesise that the reliance of other CSPs on companies that have IaaS capabilities, and the need for the IaaS providers to stand out have led to their increase in supply chain transparency.

As for IT industry certification, most of the SaaS providers who also ran an IaaS service, had and published their accreditations, with the least CSP being ISO 27001 certified, while most others had a long list of industry accreditation including ISO9001, PCI, Cyber Essentials, N3 ISP certifications. Amongst the other SaaS providers, only huddle and kahootz, both of which are collaboration CSPs made mention of their IT certification. We believe this is because these two vendors in

addition to working on government projects also engage in other consulting and managed services practices. There might have been a requirement placed on them to obtain the certification and on achieving it, they publish it to stand out from their competitors. Some of the other CSPs although mentioned that their service is hosted in a datacenter with some industry certifications, they do not claim to hold such certification for their particular service. We suggest that the other CSPs, who don't possess IT certifications, or who do not publish it, possibly do not need it to compete in the marketplace, or their provider's certification is enough to suffice. We conclude that specialist CSPs make enterprise-level security a priority and demonstrate that commitment with appropriate accreditation.

SLAs can be defined as a measure of how committed a cloud provider is to availability and security of their cloud service and how they plan to respond in the event of service interruptions. Interestingly, we observed that such a fundamental information was missing from some CSPs website. Again, the finance sub-group was the worst performing group of CSPs, with none of our compared CSPs having any SLA published. To verify this claim, we carried out searches using Google search techniques, looking for the word "SLA" on their websites and this did not yield any result. However, we found that, for a CSP such as kashflow, whose IaaS provider, IRIS was public, we were able to confirm IRIS's SLA, and suggest this will also apply to the kashflow service. It is also possible that the CSPs who did not publish their SLA on their website provided this information to their customer during the sign-up process. It is rather disappointing to see that such critical information, like the SLA, is left out of CSPs websites.

Turning now to the DR and monitoring capabilities of the CSPs, and the transparency of such information, providers in both online workspace and collaboration sub-group had excellent transparency scores. One of the many known advantages of using a cloud service was that a CSP could help customers with their incident response and disaster recovery as most CSP have this capability inbuilt into their service. While we believe on the average this is true; our data suggests that not all providers of cloud service prioritise disaster recovery. Our worst performing sub-groups for DR transparency were finance and CRM. One reason for the non-transparency or unavailability of such feature could be that these CSPs are relying solely on their IaaS providers to ensure availability of their service or perhaps their business needs does not include incident management or disaster recovery. While the latter could be the case, we argue that customers of such CSPs are likely to be impacted by supply chain failure, if they assume the controls are in place and make no alternative arrangement for such services.

On Architecture, the overall evidence of cloud architectures published on CSP websites was inadequate. However, we are not surprised by this trend, considering the level of abstraction that makes up most cloud architectures. Out of the 25 CSPs, we compared, only four of them provided details of their cloud architecture, three of which were IaaS providers who we might expect to provide this information to their prospective IaaS and SaaS customer. We argue that, despite the inability of clients to control their cloud infrastructure, their ability to independently verify how their data is being transferred, stored, accessed, and secured helps them with their risk assessments and decision making.

Lastly, we compared the SaaS providers based on their transparency of datacenter locations. Sixteen of the twenty-five vendors made mention of their datacenters and its location, with some more detailed than the others. A few of the CSPs just alluded to the fact that customer data was hosted in a Tier “x” datacenter in the UK, while others provided the location, and who owned the datacenters. We believe for customers to exercise their data controller rights over their data, they need to have visibility of that data, know where it is stored and how it is secured, and also policies and procedures surrounding its use.

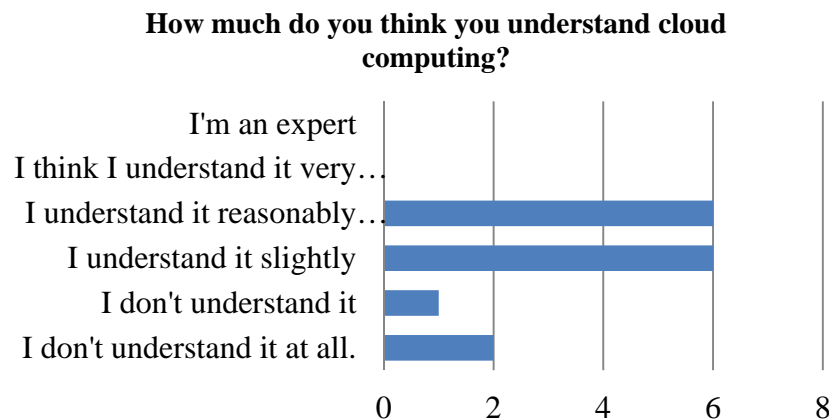
Our top performing SaaS provider, Youmanage, was the only SaaS CSP to provide their cloud architecture information, together with all other transparency feature we identified, except IT certification, which understandably they do not possess. For a start-up company established in 2010, and with less than ten employees, they are the model of what a transparent SaaS provider service should emulate. They seem to have collaborated with their IaaS provider, Pulssant, to implement a comprehensive solution, which from looking through their website, any prospective customer will be confident of their abilities, which automatically lowers customers perceived risk (see Annexe C for a description of each of the CSPs). Their enterprise cloud datasheet provides specifics about their cloud service, their processes and the support available to customers. It is not surprising to see that world-leading organisations rely on Youmanage for their HR functions.

In conclusion, and to answer our fourth research question, we assert that transparency is not a black or white situation, which is evident in our comparison, considering different organisations approach transparency in distinct ways. We discovered that SaaS providers who offered IaaS services were more transparent than regular SaaS vendors. Mainly, we found that vertical industry specific CSPs concentrate on their product and its functionality, and provide little detail on the supply chain and the security of the product. Our analysis of this vertical industry trend is in threefold, and one is that the SaaS providers do not have enough information on how their service is being provided and have completely outsourced technical control of the infrastructure to their IaaS provider. The second is that the CSP wrongly assumes that their customers are not interested in the security and availability of their data. Thirdly, it might just be that they omitted this information from their website, but are willing to share it with prospective customers at any point. We agree with Fischer-Hübner et al. (2014), on their suggestion that complex supply chain information should be provided in layers, and argue that the eight transparency features we identified can be used as a starting point for all CSPs. We believe that this information would not impede the CSPs competitive advantage, neither would it violate their intellectual rights.

#### **4.6 Supply chain questionnaire to verify CSP comparison result**

The aim of this section is to confirm our thoughts on cloud provider’s transparency about their supply chain, as evidenced by the information they publish on their websites. The opportunity to work with the MBA students of Said Business School (SBS) enabled us to assess how business leaders and non-technical consumers perceive the transparency issues in cloud computing. Out of the fifty MBA students we requested to take part in this survey, only 15 completed their questionnaire, giving us a response rate of 30%. The respondents also had a varied knowledge of cloud computing, which is representative of some small businesses, or even larger

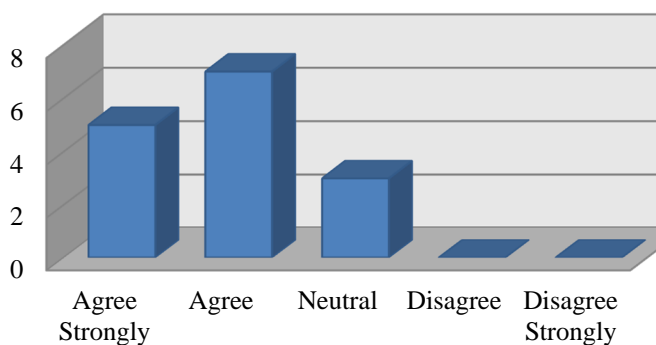
companies where the individual teams, for example, HR or Finance, have signed up for a cloud service without proper management oversight. The respondents rating of their cloud computing knowledge is as shown below:



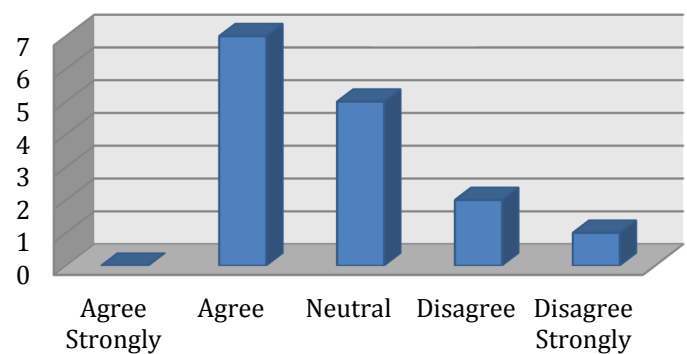
**Figure 4:** Cloud knowledge of the MBA respondents

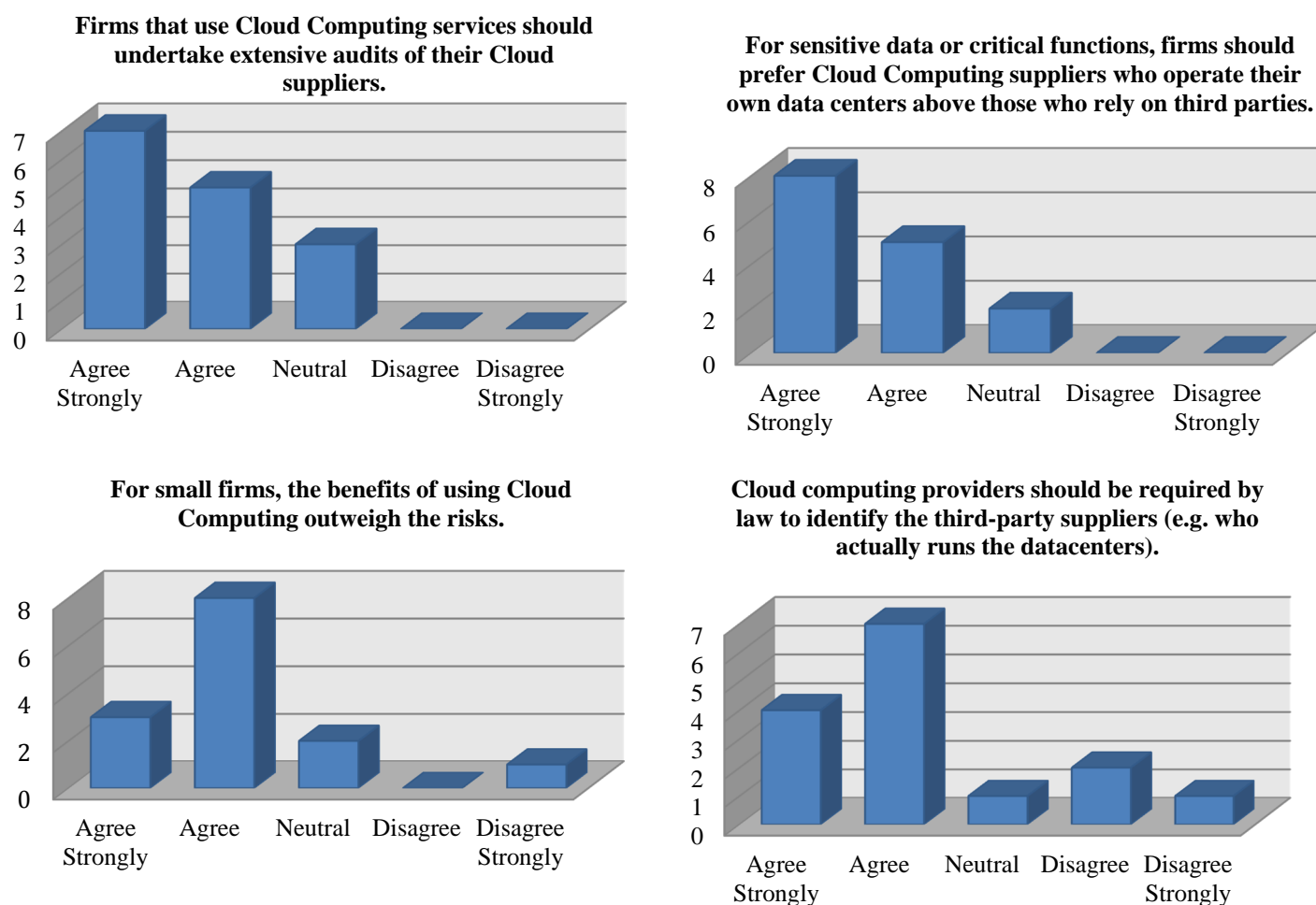
Although the students were not cloud computing experts, the majority of them had an idea, with only three out of the 16 respondents, not having an understanding of the cloud. That said, these students have been taking a supply chain module for seven weeks before the questionnaire, so we believe their knowledge of supply chain is much better than that of cloud computing. As such, we ask them a series of questions about cloud suppliers and supply chain (see Annexe C for the questionnaire). They had to choose one of 5 options in a Likert-scale (*Agree Strongly*, *Agree*, *Neutral*, *Disagree* and, *Disagree Strongly*) and their responses to the questions asked are shown in the figure3 below:

**Firms that purchase cloud services should only contract with firms that provide explicit information about the 'supply chain' that sits behind the cloud service.**



**For large firms, the benefits of using Cloud Computing outweigh the risks.**





**Figure 5: Benefit vs. Risk of cloud supply chain**

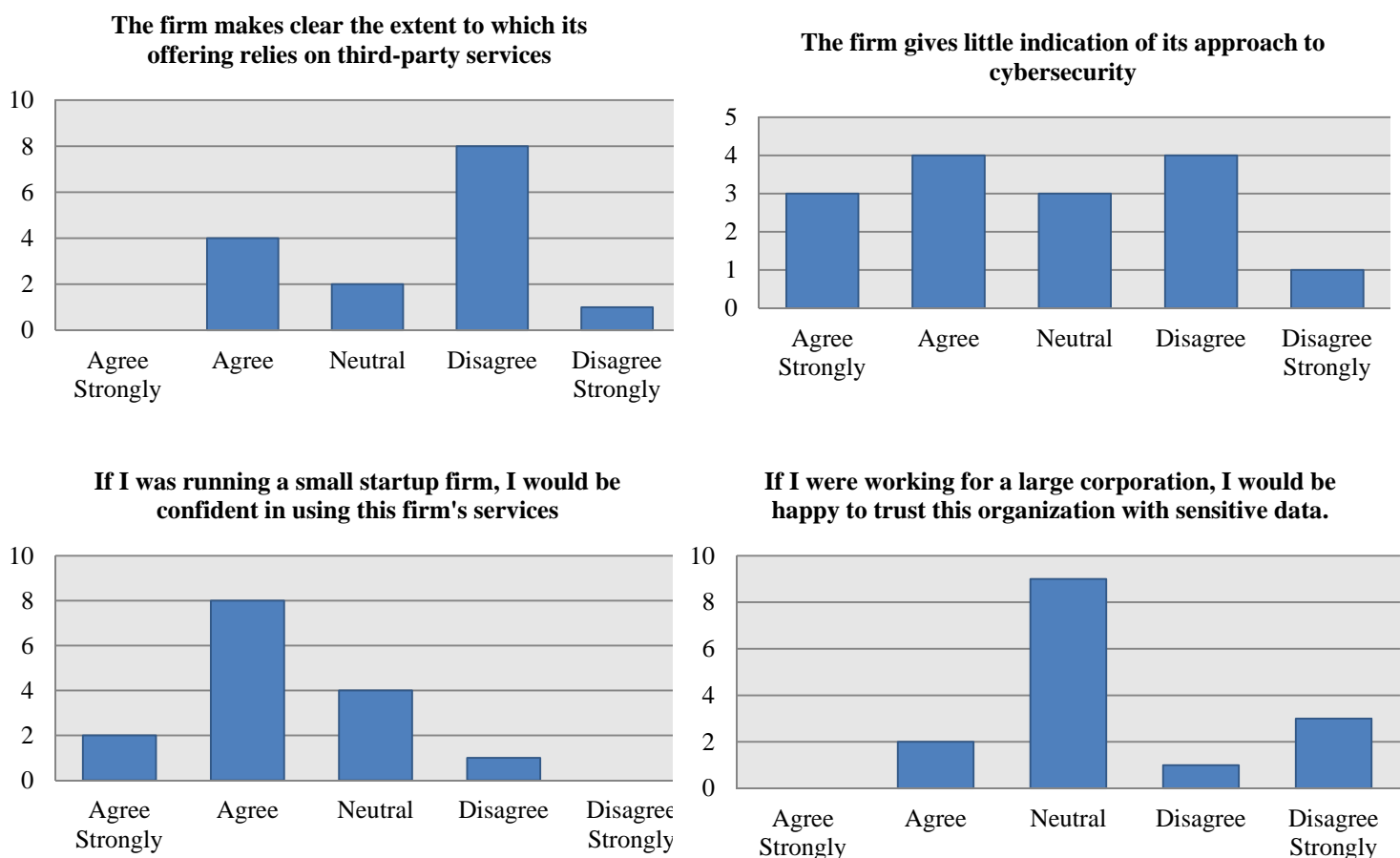
From the data in Fig3, we see that the respondents overwhelmingly supported purchasing cloud service from CSPs who provided explicit information about their supply chain. Likewise, there was a good support for the argument that cloud providers who hosted their cloud infrastructures were at a lower risk of supply chain failure than those who outsource to 3rd parties. We like to draw attention to the question of benefits vs. risk, for both small and large organisations. The respondents agreed that for both cases, the benefit of cloud outweighs the risk, with the small businesses receiving stronger support for benefits over risk. This result is explained by the fact that with traditional IT, SMBs have struggled to access the needed expertise at a reasonable price that can keep them in business, but the cloud, not only provides a viable solution, it significantly boosts their productivity (BCSG, 2015).

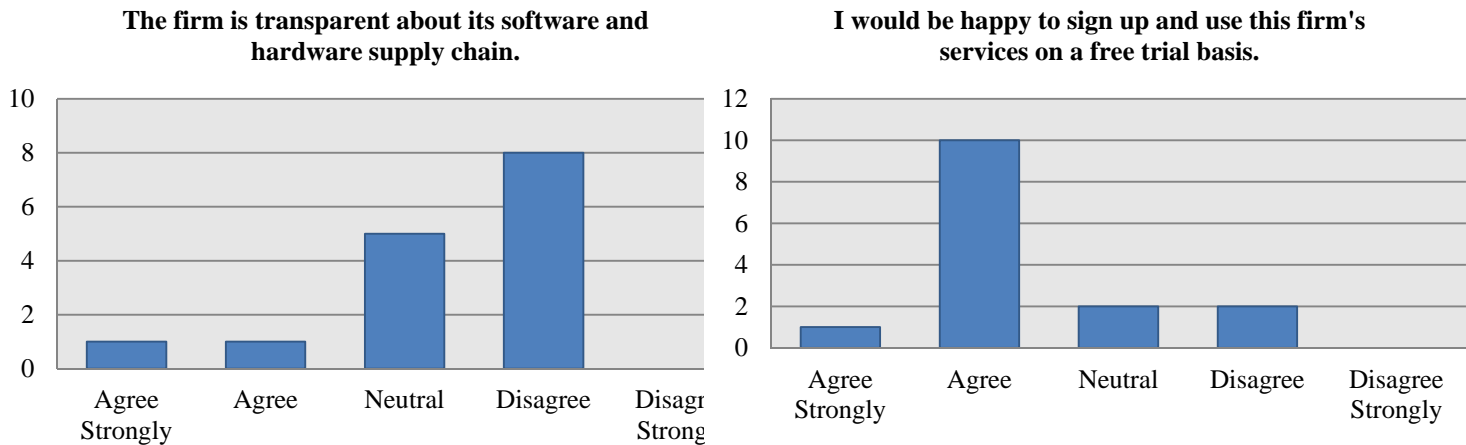
We deliberated if CSPs and IT providers in general, should be required by law to identify their third-party suppliers, and we put this question to the respondents. A majority of them (11) agreed with this proposition, while three respondents disagreed, with one staying neutral. Regulators of the food and health care industry, with the support of the government, have mandated supply chain transparency, because of its implication on the health of the populace. Perhaps, such regulations should be brought into the IT industry, to help sustain businesses from collapsing due to increased risk of supply chain failure.

After the initial questions probing the thoughts of the respondents on cloud providers and supply chain, we proceeded to ask the respondents to investigate some cloud vendors and give their assessment of the supply chain transparency exhibited by each of those vendors. Each of the respondents was tasked with analysing one of six websites that were randomly selected by the researcher. The CSPs websites are as follows:

- *glisser.com*
- *prezi.com*
- *cleaside.com*
- *spideroak.com*
- *onfido.com*
- *workday.com*

To aid the respondents investigation, we listed six questions for them to use in providing feedback of their opinion on the providers website and also gave them an opportunity to provide us with an overall feedback of their judgement of the transparency the firm's cloud supply chain. The responses of our participants are as contained in figure 4 below.





**Figure 6:** Assessment of CSPs by MBA respondents

The response to the initial question on CSPs transparency shows the limited amount of information these providers published on their website, which confirms the researchers initial assessment of the 25 SaaS providers earlier analysed. Although this is the current state of affairs with regards to supply chain transparency, the respondents favoured using the service both for a free trial and as a start-up company. This result would seem to be expected when we consider that many users sign up for the functionality (benefits), and do not necessarily dwell on the risk element, which might include SaaS providers using customer records for advertisement and marketing purposes. The advantage of the cloud includes its ability to regularly deliver new enhancement and the pay-per-use pricing, which makes budgeting predictable and manageable for start-ups (Columbus, 2016). However, the feedback for the use of this CSPs service in a large corporation was more neutral, leaning towards a negative response. Large organisations are known to be risk-averse and are wary of entrusting their mission-critical or productive applications to a cloud provider who they are not assured of its high standards, availability, supply chain or SLAs.

Some of the general feedbacks from the respondents about the transparency of the cloud providers are as follows:

*“Not transparent - uses general statements, but gives no detail.”*

*“The security documentation is decent... it is fairly transparent if you spend a while and look for information that you need.”*

*“Transparency is not their main selling point or what they want to focus on (but rather the efficacy and functionality of the tool).”*

*“Not much, but on the other hand, it's not necessary by nature of their offering.”*

*“They seem to be taking a very simplistic approach on their offer. It looks as it's targeted towards people who don't quite know how this works but want to collect its benefits.”*

The respondents made the above, and many more statements in the same fashion about the supply chain transparency of the CSPs. A good point to reiterate is the

vertical industry-specific providers, who just provide details on the functionality of the product and do not try to “overwhelm” their potential clients with what's behind the cloud, even though is important. We argue that is important for CSPs to have a baseline of supply chain information that they need to publish on their websites, which can assist customers in assessing their risk of using such service. Customers who do not need the information can ignore it, but it is readily available for those that require it.

In conclusion, our research has shown that there seems to be the right supply chain for every cloud product. How CSPs choose to be transparent with such information is a strategic decision at the board level. So, we decided to ask respondents if they were happy to reveal the identity of their third-party suppliers and what issues would determine their approach? Here are some of their responses:

*“That could kind of give away some of my competitive advantages....”*

*“...my customers can get insights to my cost structures and my competitors might try to mimic my supply chain or undermine it.”*

*“I would, as transparency on this matter I believe can be made into a unique selling point (USP).”*

*“Not at all happy. Part of the business model would be to identify the lowest cost solution with the minimum standards met.”*

*“Happy to maintain transparency and build trust.”*

*“Servers on shadier locations with poorer data protection laws could cause some bad rap, which might incline the providers to reveal less of that.”*

*“...depending on the brand reputation of the third party service provider.”*

Although the respondent’s feedback is a summary of both sides of the CSP transparency argument, it is unsurprisingly swayed towards CSPs making a profit for their business. Many of the respondents are willing to maintain the profitability of their businesses, even if it means less transparency of the supply chain. We argue for the increase in transparency at any cost, because as we have seen throughout this study, it boosts cloud customers trust in the service, their ability to assess risk and put mitigation plans in place while remaining productive. A CSP that is transparent with its supply chain could develop a USP that will drive more customers to them. We are aware of the genuine risks that can result from supply chain transparency but argue that the fact that companies know that they need to be transparent with their chain will influence them in choosing quality partners, who they can work with the achieve great products.

## **5. Conclusion and Future work**

In this study, we set out to determine the effect of transparency in reducing supply chain risks in cloud computing. Cloud computing is a combination of benefits and risks. The delivery of a cloud service is rooted in an inherently complex and dynamically formed cloud provider chain. This complexity of cloud supply chain, made up of sub-tiers of multiple suppliers, increases cloud risk in a way that makes it

unlikely to be mitigated by contractual clauses with the CSP. In this study, we found that cloud-adopting organisations failed to address their cloud risks in their ERM, and many of them do not have a clearly defined risk appetite. From the risk assessment results, we were able to establish the extent to which cloud supply chain transparency helped to reduce the risk of cloud adoption. With varied results among the CSPs we assessed, we found out that customers awareness of providers processes and controls together with increased visibility into the vulnerability of the chain, helps them to foresee challenges and enable a proactive response to resulting threats. Also, we found out that although there was an incentive for cloud providers to be transparent with their supply chain, not least to gain the trust of their customers, some CSPs refrained from doing this for the sake of maintaining profitability, protecting intellectual property and competitive advantage. Some of the identified reasons for the vague information on supply chains include:

- CSPs are not aware of their supply chain beyond the first tier.
- Cloud customers favour the functionality and cost of a cloud service over its provenance.
- CSPs are uncertain about the quality and quantity of technical and supply chain information to share with their customers.

We mainly observed a lack of transparency among the CSPs that provided services for the vertical market such as financial industry and noticed that providers of infrastructure services (IaaS), provided more detailed information about their supply chain than the typical SaaS provider. This might be due to the diverse customer base of IaaS providers, which included both end-customers, as well as SaaS and PaaS providers. We established that an improved communication within the supply chain and transparency into the adequacy of the internal controls provided trust in operation, confidence and adequate understanding of residual risk.

To address the quality and quantity of information CSPs should share with their customers, we identified eight transparency features (security controls, architecture, SLA, DR/BCP, IT certification, technology partners) that we firmly believe should be made available to prospective and current customers. We used these features to compare 25 SaaS providers cut across five cloud service categories and concluded that although each provider approached supply chain in a different way, customers develop confidence in the services of providers that were upfront with detailed information on these transparency features. We conclude that, although cloud supply chain is not a black or white situation, it is ultimately customer-driven and could soon become a competitive differentiator for cloud service providers, especially SMB providers.

Despite its exploratory nature, this study has gone some way towards enhancing our understanding of cloud provider chains and the thoughts and action of cloud providers concerning supply chain transparency. Whilst not conclusive, this study makes a significant contribution to addressing: (i) the nature of supply chain information CSPs can share with their customer while still maintaining their competitive advantage; (ii) the level of information vertical and horizontal market CSPs currently publish on their website; and (iii) the importance of the supply chain awareness and the visibility of third party risks to effective risk management. However, the major limitation of this study is its ability to generalise to the wider cloud provider community due to the

number of respondents that participated in each of the phases. Also, we were not able to comprehensively assess the risks of cloud customers concerning their supply cloud chain, and so are unable to generalise the impact of supply chain disruptions on cloud operations.

For our future work, we would be expanding on our cloud comparison study to include PaaS and IaaS vendors, as well as increase the transparency features, with each feature having a different weighting that can be fed into an algorithm to calculate the overall transparency of a CSP. The inclusion of IaaS and PaaS providers in this comparison would be to investigate if indeed there is a pattern of supply chain transparency with the different service models, or perhaps it is ultimately down to the strategic decision of the management of each CSP. We will undertake a systematic random sampling of the UK cloud computing provider's directory, expecting to identify 100 cloud providers that we can assess. Our choice of UK providers is down to convenience and proximity to the research team, in cases where we need to visit the companies as part of the research work. In measuring transparency, we would focus on how much information the CSPs reveal and how easy it is to access this information. As we noticed in our just concluded study, CSPs sometimes gave vague information on their security controls and architecture, but more daunting was the effort to locate this information. Since transparency and control in the cloud require more complex information about the data handling along the cloud chain, we hope to generate the optimal transparency features based on input from a group made up of 20 or more respondents, made up of UK cloud providers and customers. We will be leveraging our existing relationship with cloud providers to expand the network to their clients and partners using the snowball sampling technique.

Furthermore, according to Fisher et al. (1997), there is a right supply chain for every product, from functional to innovative, as well as BAU and strategic. Therefore, we hope to develop a framework that can help providers formulate the best supply chain strategy for their offering, and determine the level of transparency applicable to each arrangement with a capability of improving their overall performance. We aim to investigate how different supply chain arrangements assist CSPs to offer secure and reliable services, introduce a steady stream of innovations, predict demand, maximise profit, and remain viable, while meeting customer needs. Further studies need to be carried out to validate why vertical industry specific CSP, have so far shared less information about their supply chain. Our aim is to engage with non-transparent cloud providers in the vertical markets to try to understand the reason behind the trend and suggest our transparency features to them if they are open to change.

Lastly, we aim to carry out comprehensive risk assessments of small, medium and large organisations based on their supply chain risks that stem from cloud computing. Building on the established trust with our participants, and given enough notice, we hope to assess the risks of at least five of these firms using the OCTAVE Allegro risk assessment methodology. OCTAVE Allegro is considered the methodology of choice because of its flexibility and weighted scoring system that provides a quantitative comparison for threat prioritisation and asset valuation.

### **Acknowledgements**

I would like to thank EPSRC for funding this research work. Also, special thanks go to my supervisor, Dr Steve New for his excellent support, guidance and encouragement through the duration of the study.

## References

- Akkermans, H., 2004. Travail, transparency and trust. In *European Journal of Operational Research*. pp. 445–456. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0377221703001644>.
- Akkermans, H., Bogerd, P. & Van Doremalen, J., 2004. Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics. In *European Journal of Operational Research*. pp. 445–456.
- Albert S., H.I. & Rajeev, A., 2015. Trust in Cloud Computing. *Ieee*, (October), pp.01–08. Available at: [http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7132885&url=http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=7132885](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7132885&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7132885).
- Ashford, W., 2013. Transparency, not security, is biggest cloud challenge, says Verizon. Available at: <http://www.computerweekly.com/news/2240185187/Transparency-not-security-is-biggest-cloud-challenge-says-Verizon> [Accessed May 1, 2016].
- Auty, M. et al., 2010. Inadequacies of current risk controls for the cloud. *Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*, pp.659–666.
- BCSG, 2015. The small business revolution: trends in SMB cloud adoption. , p.23. Available at: <https://www.bcsbg.com/wp-content/uploads/2015/03/The-small-business-revolution-trends-in-SMB-cloud-adoption.pdf>.
- Bhensook, N. & Senivongse, T., 2012. An assessment of security requirements compliance of cloud providers. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, (3), pp.520–525.
- Bilderbeek, P., 2014. CLOUDSCAPE – UNITED KINGDOM. , (February), p.2014.
- Boyens, J. et al., 2015. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Special publication*.
- Bruce Schneier, 2002. Secrecy, Security, and Obscurity.
- Butler, S. a & Fischbeck, P., 2002. Multi-Attribute Risk Assessment. *Reliability Engineering*, 94(2), pp.187–198. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.8970&rep=rep1&type=pdf>.
- Cayirci, E. et al., 2014a. A cloud adoption risk assessment model. *Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014*, pp.908–913.
- Cayirci, E. et al., 2014b. A cloud adoption risk assessment model. In *Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014*. pp. 908–913.
- Cayirci, E., 2015. *Accountability and Security in the Cloud*, Available at: <http://link.springer.com/10.1007/978-3-319-17199-9>.
- CERT-UK, 2015. Cyber-security risks in the supply chain. , p.10. Available at: <https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf>.
- Chan, W., Leung, E. & Pili, H., 2012. Enterprise risk management for cloud computing. *Committee of Sponsoring Organizations of the Treadway Commission*, p.4.
- Charney, S. & Werner, E.T., 2011. Cyber Supply Chain Risk Management : Toward a Global Vision of Transparency and Trust. , p.19. Available at:

- [http://download.microsoft.com/download/3/8/4/384483BA-B7B3-4F2F-9366-E83E4C7562D6/Cyber Supply Chain Risk Management white paper.pdf](http://download.microsoft.com/download/3/8/4/384483BA-B7B3-4F2F-9366-E83E4C7562D6/Cyber%20Supply%20Chain%20Risk%20Management%20white%20paper.pdf).
- Chopra, S. & Sodhi, M.S., 2004. Managing risk to avoid supply-chain breakdown. *MIT Sloan management review*, 46(1). Available at: <http://www.emeraldinsight.com/doi/abs/10.1108/SCM-12-2013-0474>.
- Columbus, L., 2016. Roundup Of Small & Medium Business Cloud Computing Forecasts And Market Estimates , , pp.1–9.
- Conley, R., 2012. Three Levels of Trust – Where Do Your Relationships Stand? | Blanchard LeaderChat on WordPress.com. Available at: <http://leaderchat.org/2012/10/25/three-levels-of-trust-where-do-your-relationships-stand/>.
- Council, C., 2015. Security for Cloud Computing 10 Steps to Ensure Success. , pp.1–35.
- CPNI, 2015. SECURITY FOR INDUSTRIAL CONTROL SYSTEMS- Manage Third Party Risks.
- Das, T.K. & Teng, B.-S., 2001. Trust, Control, and Risk in Strategic Alliances: An Integrated Framework. *Organization Studies*, 22(2), pp.251–283.
- Demsash, B.G., 2012. Framework To Adopt Cloud Computing for Medical Image Archiving and Sharing. , (BIZUAYEHU), p.144.
- Dziminski, B. & Gleeson, N.C., 2015. Accountability and Security in the Cloud: First Summer School, Cloud Accountability Project, A4Cloud, Malaga, Spain, June 2-6, 2014, Revised Selected Papers and Lectures. In M. Felici & C. Fernández-Gago, eds. Cham: Springer International Publishing, pp. 226–247. Available at: [http://dx.doi.org/10.1007/978-3-319-17199-9\\_10](http://dx.doi.org/10.1007/978-3-319-17199-9_10).
- ENISA, 2009a. An SME perspective on Cloud Computing. *Main*, p.16.
- ENISA, 2009b. Cloud Computing - Benefits, Risks and Recommendations for Information Security. *Computing*, 72(1), pp.2009–2013. Available at: <http://www.springerlink.com/index/R357K80TP72R7121.pdf>.
- ENISA, 2006. Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools. , (June), p.177. Available at: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools>.
- Felici, M. & Pearson, S., 2015. Accountability and Security in the Cloud: First Summer School, Cloud Accountability Project, A4Cloud, Malaga, Spain, June 2-6, 2014, Revised Selected Papers and Lectures. In M. Felici & C. Fernández-Gago, eds. Cham: Springer International Publishing, pp. 3–42. Available at: [http://dx.doi.org/10.1007/978-3-319-17199-9\\_1](http://dx.doi.org/10.1007/978-3-319-17199-9_1).
- Fischer-Hübner, S., Angulo, J. & Pulls, T., 2014. How can Cloud Users be Supported in Deciding on , Tracking and Controlling How their Data are Used ? , 1983, pp.77–92.
- Fisher, M.L., Day, G.S. & Ryan, W., 1997. What is the Right Supply Chain for Your Product ? *Harvard Business Review*.
- FT Lexicon, Supply Chain Transparency Definition from Financial Times Lexicon. *Financial Times*. Available at: <http://lexicon.ft.com/Term?term=supply-chain-transparency> [Accessed May 11, 2016].
- Gadia, S., 2011. Cloud Computing Risk Assessment: A Case Study. *ISACA journal*, 4, pp.11–16. Available at: <http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx>.

- Garg, S.K., Versteeg, S. & Buyya, R., 2012. A framework for ranking of cloud computing services. *Future Generation Computer Systems*, 29(4), pp.1012–1023. Available at: <http://dx.doi.org/10.1016/j.future.2012.06.006>.
- Hofstede, G.J., 2002. *Transparency in netchains*, ISACA & CSA, 2015. Cloud Computing Market Maturity. *AN ISACA CLOUD VISION SERIES WHITE PAPER*, pp.1–12.
- ISO 27005, 2011. BS ISO / IEC 27005 : 2011 BSI Standards Publication Information technology — Security techniques — Information security risk management.
- Jeff Lowder, 2008. The Difference between Quantitative and Qualitative Risk Analysis and Why It Matters.
- Kaliski-Jr, B.S. & Pauley, W., 2010. Toward Risk Assessment as a Service in Cloud Environments. *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, pp.1–7.
- Kleindorfer, P.R. & Saad, G.H., 2010. Managing Disruption Risks in Supply Chain. , 14(1), pp.434–438.
- Lamming, R.C. et al., 2002. Transparency in supply relationships: Concept and practice. *IEEE Engineering Management Review*, 30(3), pp.70–76.
- Leimeister, S. et al., 2010. The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks. *Proceedings of 18th European Conference on Information Systems ECIS 2010*, (Ecis 2010), pp.1–12.
- Lewis, R. et al., 2014. Cybersecurity Information Sharing : a Framework for Information Security. *Twenty Second European Conference on Information Systems*, pp.1–15.
- Li, A. et al., 2011. Comparing Public- Cloud Providers. *IEEE Internet Computing*, 15(2), pp.50–53. Available at: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5731587](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5731587).
- Lynn, T. et al., 2013. The case for cloud service trustmarks and assurance-as-a-service. *CLOSER 2013 - Proceedings of the 3rd International Conference on Cloud Computing and Services Science*, pp.110–115. Available at: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84884472388&partnerID=40&md5=8ab242df97da635e2b177ee3a92e0f80>.
- Marston, S. et al., 2011a. Cloud computing - The business perspective. *Decision Support Systems*, 51(1), pp.176–189.
- Marston, S. et al., 2011b. Cloud computing — The business perspective. *Decision Support Systems*, 51(1), pp.176–189. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0167923610002393>.
- Microsoft, 2015. Trusted Cloud : Microsoft Azure Security , Privacy , and Compliance. , (April).
- Myers, M.D. & Newman, M., 2007. The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1), pp.2–26.
- New, S., 2009. Supply chain traceability and product provenance : challenges for theory and practice.
- New, S. & Brown, D., 2012. The Four Challenges of Supply Chain Transparency. *European Business Review*, pp.1–7. Available at: <http://www.europeanbusinessreview.com/?p=4082>.
- Pearson, S. et al., 2012. Accountability for cloud and other future Internet services. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, pp.629–632.
- Pohlman, M., 2010. Using the CSA Control Matrix and ISO 27017 controls to facilitate regulatory compliance in the cloud. *Cloud Security Alliance*. Available

- at:  
[http://docbox.etsi.org/workshop/2012/201201\\_SECURITYWORKSHOP/3\\_INTERNATIONAL\\_STANDARDIZATION/EMC\\_CSA\\_POHLMANN.pdf](http://docbox.etsi.org/workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/EMC_CSA_POHLMANN.pdf).
- Raj Samani, 2011. Common Assurance Maturity Model. , pp.1–2.
- Raymond, L. & Renzetti, C., 2015. The problem of researching sensitive topics.
- Remus, W., 1986. Graduate students as surrogates for managers in experiments on business decision making. *Journal of Business Research*, 14(1), pp.19–25.
- Reuven Cohen, 2013. New Cloud Computing Insurance Attempts to Solve Cloud Liability Concerns For Service Providers.
- Rousseau, D.M. et al., 1998. Not so different after all: A cross discipline view of trust. *Academy of Management Review*, 23(3), pp.393–404.
- Schlegel, B.G.L. & Trent, R.J., 2012. Risk management : Welcome to the new. *Logistics Management*, (2), pp.42–45.
- Schneier, B., 2008. The Psychology of Security Bruce. , (Part 1), pp.1–14.
- Sheppard, B. & Tuchinsky, M., 1996. Trust in Organizations: Frontiers of Theory and Research. , 8(2), pp.140–165.
- SSAE, 2016. SOC 2 Report – Trust Services Principles.
- Sunyaev, A. & Schneider, S., 2013. Cloud Services Certification. *Communications of the ACM*, 56(2), pp.33–36. Available at:  
<http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=88140957&site=ehost-live&scope=site>  
<http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iuh&AN=88140957&site=ehost-live&scope=site>.
- Talluri, S., Narasimhan, R. & Nair, A., 2006. Vendor performance with supply risk: A chance-constrained DEA approach. *International Journal of Production Economics*, 100(2), pp.212–222.
- Verbano, C. & Venturini, K., 2013. Managing Risks in SMEs: A Literature Review and Research Agenda. *Journal of Technology Management & Innovation*, 8(3), pp.186–197. Available at:  
<http://eserv.uum.edu.my/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=94732827&site=ehost-live&scope=site>.
- Vijayan, J., 2015. Cloud Security: Transparency Is Crucial for Service Providers. *CIO*. Available at: <http://www.cio.com/article/2925773/cloud-security/cloud-security-transparency-is-crucial-for-service-providers.html> [Accessed May 9, 2016].
- Weber, R.H. & Staiger, D.N., 2014. Cloud Computing: A cluster of complex liability issues. *Web Journal of Current Legal Issues; Vol 20, No 1 (2014): Web JCLI*, 20(1), pp.1–13. Available at: <http://webjcli.org/article/view/303/418>.
- Werff, L. Van Der, Lynn, T. & Xiaong, H., 2014. Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label. *ICDS 2014, The Eighth ...*, (c), pp.157–163. Available at:  
[http://www.thinkmind.org/index.php?view=article&articleid=icds\\_2014\\_6\\_40\\_10104](http://www.thinkmind.org/index.php?view=article&articleid=icds_2014_6_40_10104).
- Wisner, J.D., Tan, K.-C. & Leong, G.K., 2008. *Principles of Supply Chain Management - A Balanced Approach*, Available at:  
<http://www.amazon.de/dp/0324659911>.
- Zhang, X.Z.X. et al., 2010. Information Security Risk Management Framework for the Cloud Computing Environments. *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, (2007), pp.1328–1334.

**Annexe A – Risk Assessment questionnaire**

**[supply chain risk assessment](#)**

**Annexe B – Non-technical supply chain questionnaire**

**[supply chain questionnaire](#)**

**Annexe C - Description of the 25 compare SaaS providers.**

**[SaaS CSP details](#)**