A Business Analysis of Cloud Computing: Data Security and Contract Lock-in Issues

Justice Opara-Martins, Reza Sahandi, Feng Tian
Faculty of Science and Technology
Bournemouth University
Bournemouth, United Kingdom
{joparamartins, rsahandi, ftian}@bournemouth.ac.uk

***Abstract*—The widespread adoption of cloud computing services has a wide range of sourcing issues that companies must take into consideration when they standardize and automate their IT service delivery. In this respect, our paper identifies risks and opportunities of cloud computing which affect organisations' cloud adoption decisions. The research method used is based on a quantitative online survey questionnaire of 114 UK business respondents including IT professionals, managers, and decision-makers. The study results show that despite the business benefits for moving IT service consumption and delivery from on-premise to the cloud environment, the following risks are exacerbated: security, data privacy and contract lock-in. The outcome of the survey suggests that related concerns can be strategically mitigated. This can be done by negotiating cloud contracts to be more closely aligned to address business specific security and lock-in risks in cloud-based sourcing. Based on the outcome, the paper provides guidance to support the decision-making process on investment into cloud computing implementation to meet the organisations' business objectives with related concerns.**

Keywords—cloud computing security; data privacy; enterprise cloud adoption; cloud contract; contract lock-in

I. INTRODUCTION

The supply of information technology (IT) in the cloud has been enabled both by the evolution of sophisticated data centres (e.g. software defined network or SDDC) and widespread access to improved network bandwidth [1]. In essence, these technical advances mean that traditional IT services such as data storage, servers, networks etc. are hosted on physical machines across a wide range of locations. But from the business (i.e. consumer and end-user) perspective, they simply are virtualized resources residing in the 'cloud'. In other words the term 'cloud' is simply a new way in which business is done and IT is provided. Broadly speaking, cloud computing is a natural evolution of business model in IT services consumption and delivery. While it is important disambiguate the term 'cloud' for practical reasons, the rest of this paper embodies and assumes such definition. A unique business advantage of this model of IT service provision is the ubiquitous access it provides to customers to improve their ability to access applications and data from remote locations (location independence) and multiple devices (device independence). Delivered in this manner, the functionality can either be at the infrastructure level, platform or at the application level.

Currently, cloud computing services are finding more applications in business, and extensive attention in the industry. Previously, the UK cloud computing market was estimated to reach around £10.5 Billion, up from £6.1Billion in 2010 [2]. More recently, according to IDC, the UK IT market is valued at around £20Bn with cloud associated revenues growing to around 20% of that by 2015. Moreover, recent research from Cloud Industry Forum [3] suggests that by the end of 2015, over 90% of UK organisations (up from 78% in 2014) will have formerly adopted at least one cloud service. Furthermore, according to the research reported in this paper, over 50% of UK businesses are already using cloud services, while a greater majority (69%) utilise a combination of cloud services and internally owned applications (hybrid IT) for organisation needs. While research confirms the widespread adoption and usage of cloud computing services across enterprises, arguably it could be said primarily of cloud computing as a business phenomenon rather than a technological one.

Despite the numerous advantages of cloud computing to organisations, from the business perspective, a number of challenges such as security, data privacy, and contract lock-in remain inadequately addressed. In this paper we aim to address these issues of concern and implications to UK business cloud adopters. Thus, the study presented here provides a concise yet relevant discussion and analysis of these issues with some fundamental guidelines that should be observed by organisations, entering into a cloud computing service contract. The survey study of 114 UK respondents including IT professionals, managers, and decision-makers, shows that as computing resources move from on-premise to the cloud environment, the issues identified above are exacerbated. This further complicates decision making for/or against cloud adoption. Therefore, addressing these issues has the potential to contribute substantially to the growing body of knowledge on cloud computing. In essence this paper deals with: (1) Security, data privacy, and contract lock-in issues in cloud computing, (2) Analysis of effective strategies to protect enterprises from identified risks and concerns, using the cloud computing service contract.

Cloud computing enables the transformation of IT services into standardized and automated IT delivery to meet the needs of many organisations [15]. Since that using cloud computing technology to deliver enterprise services is not without pitfalls, organisations need to understand the implications upfront so as to take full advantage of the benefits of cloud infrastructures.

On this point, we discuss a number of factors (technical and organisational) worth considering to enable enterprises (small or large) enhance their security posture, identify and mitigate privacy-specific control issues, whilst maintaining the flexibility to easily switch cloud providers (i.e. avoid lock-in) to increase IT agility and business continuity. The rest of the paper is structured as follows. Section 2 presents the methodology applied in this study. Section 3 outlines the key findings. Section 4 provides discussion and implication of findings, followed by conclusion and future work in Section 5.

II. Research Methodology

This study seeks to identify and evaluate the risks and opportunities of cloud computing which affect stakeholders' decision-making about adopting cloud solutions with regards to security and contract lock-in. The research method used in this study is based on Survey Monkey, a quantitative online survey questionnaire tool [4]. The target population consisted mainly of large corporations and small to medium-sized enterprises (SMEs) situated in the UK. Participants in the survey varied between IT professionals, managers and decision-makers within their respective business enterprise.

A total of 200 companies were invited to participate in the survey. Overall, 114 participants completed the online survey, which constituted an acceptable total response rate of 63%. Before presenting the findings for discussion, it is mandatory to explicate that the questionnaire comprised of many questions, however only those which revealed important issues of security, data privacy and contract lock-in are presented and discussed in context.

For the purpose of analysis, Table 1 presents a socio-demographic profile of the companies and participants in the survey.

TABLE I. Socio-Demographic Profile of Participant Organisation

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

III. Findings

This section presents key findings on security and data privacy risks likely to arise in an organisation using cloud computing technology. Moreover, it presents lock-in contractual issues identified by participants that contribute in exacerbating the impact of these security risks when a cloud service is in operation.

A. UK business perception of Cloud Security and Data Privacy Risks

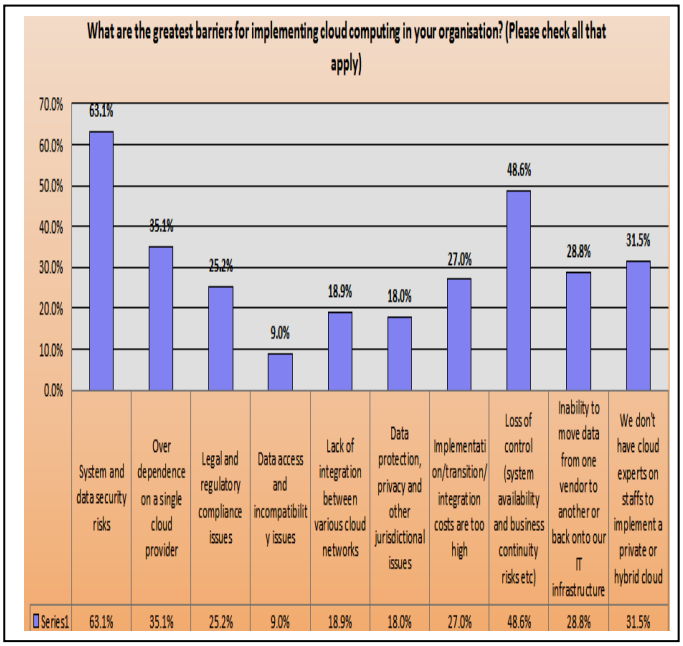

Fig. 1. Security is a top challenge for UK Cloud adopters

Fig. 1 shows majority (63.1%) of UK businesses are predominantly concerned with the security risks that can result from cloud-based solutions. In essence, these risks are partly related to general concerns arising from loss of user control and complications with data protection laws. For instance, in regard to whether geographical location matter to where organisations' data was required to be stored, 64% of respondents in the survey confirmed location mattered somewhat, 18 per cent claimed location completely mattered. Moreover, the preference of organisations (15%) who believed location did not matter at all can be explained by company's specific need regarding location of data centres and security of cloud storage (refer to Fig. 2). Generally speaking in cloud computing, data protection and data confidentiality are seen as top concerns in respect of data protection law.

One of the most legally raised concerns about cloud computing security, for businesses, is that corporate data may be stored and processed in a totally different, and potentially unknown jurisdiction. In part, this is due to loss of control which can incite legal and jurisdictional issues. Taking the organisations in this study for example, the intrinsic nature of cloud computing can impact on the information governance and compliance with UK legislation [5]. This increases the complexity associated with meeting legal and regulatory requirements for sensitive information.

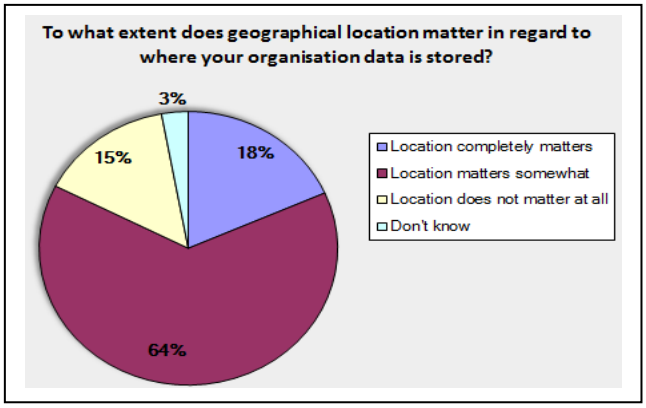

Fig. 2. Location of data centres raises jusrisdictional issues for UK firms.

Reflecting on the security and data privacy risks of putting organisations data in cloud storage, Fig. 3 shows a vast majority (60.2%) of UK business respondents claiming to be fairly concerned. About 29% admittedly are very concerned, although a lesser minority of businesses are not very concerned at all (10.7%). As well as location, the ubiquitous nature of cloud raises questions about the extent to which data is protected in transit.

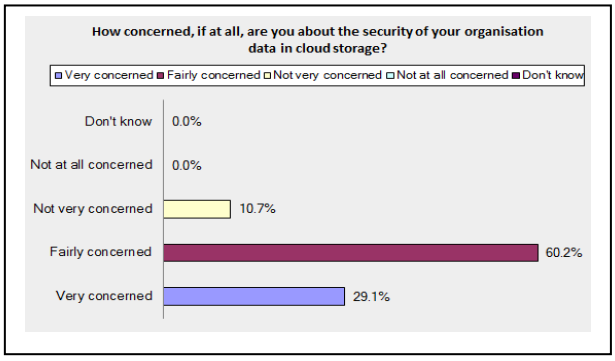

Fig. 3. Cloud storage security risks affects UK firms

This study also investigates how locations of data centres influence security concerns of UK businesses. Data analysis in Fig. 4 suggests most organisations (3.5%) still consider it safest to have their data stored with a cloud provider located in the UK, whilst (3.36%) preferred data not necessarily be located in the UK but have to be within European Economic Area (EEA). Some organisations, however, still consider it safest to have their data stored on their own hardware in a shared data centre (colocation facility). Overall, interestingly, a vast majority believe locating their corporate data anywhere in the world is unsafe. In other words, the findings indicate that some organisations perhaps operate in a regulated environment where issues with data security, data protection and data privacy laws impact the deployment options available to them. In other words regulatory issues related to security and data privacy risks vary with jurisdiction. This seems unsurprising as data protection law is horizontal rather than vertical, meaning it regulates all sectors, and controllers of personal data remain responsible if processing data in the cloud [6].

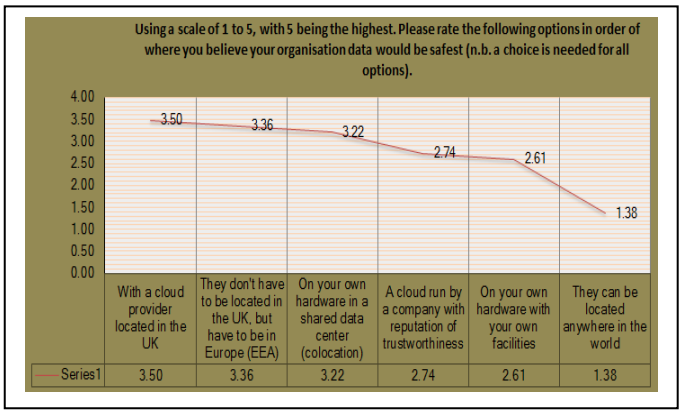

Fig. 4. Enterprises prefer corporate data stored within the UK

B. *Contract Lock-in issues*

From a business perspective, there is more than one way to get locked-in to a cloud vendors system; an often overlooked method is through a contract. Wang in [7] believes there are three reasons why businesses face vendor lock-in: limited rights and controls for users, ambiguous and ultimately expensive switching costs and vendor complacency. Cloud computing providers can create lock-in through contractual terms, or through the physical holding of customer's data. In this regard, there is an economic benefit to the vendor in the form of a regular revenue stream, but not so much of business benefits to consumers. From a commercial perspective this puts the vendor in the position of strength when it comes to renegotiate the commercial terms of agreement. For this reason, it is important not only to review the contract before signing but also negotiate the Service Level Agreement (SLA) around crucial elements like data ownership and termination conditions protecting against risks of vendor lock-in. As shown in Fig. 5**,** just one third of UK businesses in the study had the opportunity to negotiate their cloud service contracts; more than half did not negotiate while a smaller minority were unsure.

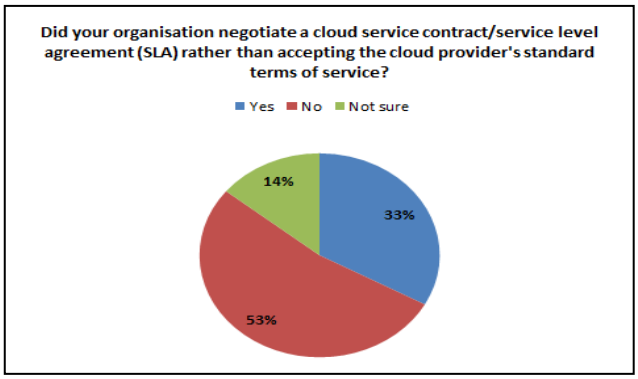

Fig. 5. Negotiated cloud contracts

However, when conducting further analysis across different organisation it becomes apparent that the rationale for those who negotiated and those who did not covers a wide variety of concerns. Of course not all businesses may be able to negotiate cloud providers' terms as has been established in the survey's findings. Moreover, as with many commercial agreements

much depends on relative bargaining power. Besides, the survey findings in-depth concurs larger organisations from regulated industries had the opportunity to negotiate providers contract terms, unlike small to medium enterprises who are likely to accept the providers standard terms of service agreement. Furthermore, to understand how UK organisations plan to minimize vendor lock-in risks through contractual provisions, the survey also explored organisations' cloud exit plans. Surprisingly 24% of businesses surveyed did not have an exit plan, 41% agreed to have an exit strategy in place but with no agreed ownership rights of data that will be stored in the cloud. Only 21% claimed they did not have an exit strategy in case of cloud service termination (Fig. 6).

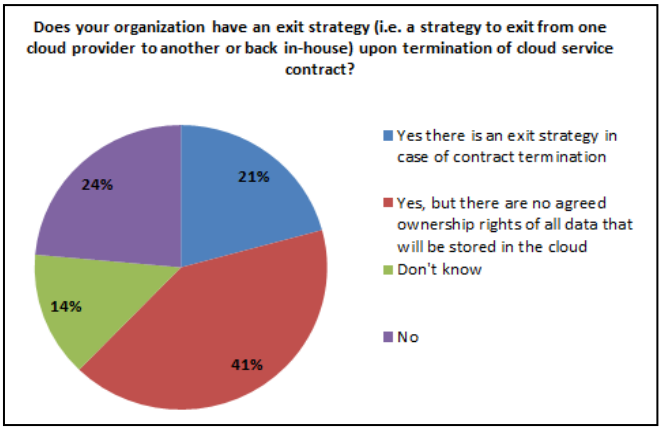

Fig. 6. Exit strategy is critical in enterprise cloud service contracts

These findings are quite surprising considering what would happen to a company, for instance, if its cloud provider goes out of business. Therefore it is important to have an exit strategy in place for each cloud type (i.e. private, hybrid etc.) or service model (i.e. IaaS, SaaS, etc.) adopted. This is essential in case of contract termination. In this case the SLA as well as the terms of conditions should be negotiated around the needs of the business. In this connection, other contractual terms identified by end-user organisations as agreements that meet their risk profiles, compliance obligations, and should be included in the contract/SLA are: right to terminate contract (80.2%), guaranteed service levels (66%), and protection and security of data (refer to Fig. 7). The findings demonstrate that, understanding the most graceful exit strategy for establishing trust should be part of due diligence when vetting potential cloud vendors or service providers. Furthermore, considering the negative impact that the contractual issues identified can have on a business, when using any cloud-based solution, it is important to ensure tools or processes are in place that can facilitate consumers to extract, access, and interchange data if such a need arises.

IV. Discussions and Implication

The objective of this section is to discuss the key findings in context by proving fundamental guidelines to UK businesses to mitigate related security and contract lock-in issues.

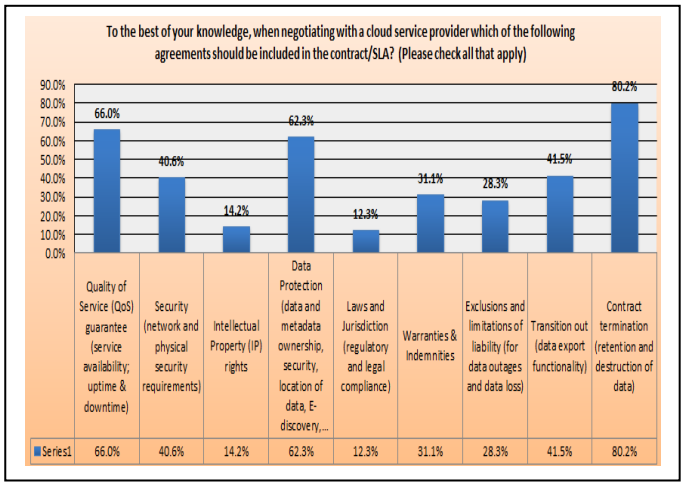

Fig. 7. Contract terms that generated most negotiation

A. *Data Security and Privacy Issues*

According to a survey conducted by International Data Corporation (IDC), 74% of IT managers and CIOs identified security as the primary challenge that hinders them from using cloud computing services. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution [2]. Likewise in this study, UK businesses have identified security as a major barrier to cloud implementation. Key references such as cloud security alliance [8] highlight different security issues related to cloud computing. Enterprises must take note of such issues in consuming cloud services. In particular issues related to data security and privacy risks should be appropriately addressed. Regulation is typically not the primary cause of these issues, though when compared to the perceived risks internal to an organisations operating environment. It can be safely deduced from these figures (see Fig. 2 & 3) that many organisations in the study are cautious about the implications and conditions surrounding their accountability to legal obligations such as Data Protection Act (DPA) [14]. The DPA in the UK for instance, applies to personal data that is processed; processing is likely to include most of the operations that are likely to occur in the cloud, including storage of data [9]. In this respect, employing an information asset management system will essentially provide the necessary level of controls to ensure sensitive information is protected and meets enterprise compliance agreement [10].

The provision of cloud services very often requires processing of data in servers located outside ones jurisdiction. Cloud computing implementation is subject to local physical threats as well as external threats. As a further matter, UK organisations moving corporate data and placing them in cloud storage environment must consider the following three core information security objectives [11]: confidentiality, integrity, and availability. These are essentially relevant as they are deemed high-priority business concerns. Common solution for achieving confidentiality can be encryption using cryptography. In terms of integrity, considering most business models rely on IT for core functionalities and processes and, thus mission critical data integrity and availability must be ensured. Since moving data to the cloud incurs loss of control over redundancy, location, dependency on provider for support,

and other relevant configuration. This leads to the need of sufficient SLA to address related security concerns and data privacy issues. This includes support for portability such that customer can take action to change cloud service provider when needed to satisfy availability, confidentiality, and integrity.

Referring to Fig. 4, the result suggests businesses are not concerned about the co-location data centre within the country so much as global data centres. Verifying that data are actually processed in data centres claimed by cloud providers is difficult, technically. Admittedly, trust is a hard thing to establish in cloud computing, nevertheless cloud providers may help increase consumer trust by enhancing transparency in terms of location of data centres, as well as assisting businesses with legal compliance as they move to the cloud. Finally, in terms of security and data privacy risks, clarity and scope of the operating environment are essential factors to consider in making confident and effective deployment decisions. Thus, the emerging challenge for business stakeholders' in their respective organisations is to ensure good governance and security compliance for effective delivery across a range of in-house and cloud-based services. Education is required in this aspect, to reassure and build confidence in the cloud business model – seeing as businesses still lack sufficient knowledge about cloud-based solutions and services.

While many standards are generally relevant to the security areas of cloud computing, we recommend that UK businesses mitigate their security concerns by ensuring that cloud providers adhere to industry accepted cloud specific standards that specifically address security and data privacy issues. Moreover, by complying with such standards, in turn cloud providers engender consumer trust in moving critical systems and data to the cloud. From the business perspective, the significant value of the three information security objective, as concerns corporate data processed in the cloud, cannot be underestimated or overemphasised.

B. Contract Evaluation

The issues discussed in this section have been identified by survey respondents as high-priority business concerns worth considering when contracting with a cloud service provider.

According to [12] contractual relationship between cloud service providers and their clients is laid out in one or more documents comprising: Terms of Service (ToS), SLA, and Acceptable Use Policy (AUP). In [6] it is claimed that the starting point for cloud contracts is usually the providers' ToS – which are provider favourable (ibid). However, recent research by [13] notes distinctions in terms and conditions governing cloud service contracts: free vs paid services. Within paid services, terms and conditions typically fall into those offering standard form contracts and those subject to negotiation. Though the latter typically are limited to those perspective customers with sufficient bargaining power (as pointed out in section **3.7**), but the former comes with common challenges in that, many cloud service providers reserved the rights to change contract terms unilaterally. Moreover, as highlighted above many cloud providers' term may not be suitable to accommodate specific (especially enterprise users) requirements. Thus, some cloud users have sought changes to make the terms more balanced and appropriate to address own circumstances and meet their heightened requirements.

Prior to discussing the pre-contractual due diligence, and contract terms identified by survey respondents as requisite provisions to consider in the contract, it is worth establishing first that as with other outsourced IT provision, a good service agreement is crucial. An SLA generally details the level of service to be provided and includes mechanisms for auditing service delivery, and also a mechanism for compensating clients for underperformance. Besides, failure to meet performance level in cloud service agreements can result in significant losses and damages for a business. Thus, an SLA should reflect organisations requirements in areas such as data security, business continuity and disaster planning [5]. Moreover, one of the key observations from the research presented in this paper was that a substantial number of organisations in the survey did not negotiate their SLA and cloud service contract (refer to Fig. 5). However, opportunities may exist for these organisations' to choose providers whose contracts/SLA is negotiable. Furthermore, unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. In fact, for the UK businesses in the survey, regarding strategy to manage potential risks of lock-in at the contract level, 80.2% of respondents said contract termination (i.e. retention and destruction of data), quality of service (QoS) guarantee (66%), and data protection (including data and metadata ownership) agreements (62.3%) should be drafted in the cloud service contract. Perhaps, these terms should be included within the contract in plain and intelligible languages. In the light of such results, it should be underlined that the impact of lock-in effect could be instantiated by the provider using proprietary data formats and service interfaces. This renders interoperability and portability of data and services difficult. For this reason, it is recommended that businesses ensure whether and how cloud providers support data portability and interoperability – prior to signing the cloud service contract. Additionally, there are standardization efforts that specifically address lock-in issues in the cloud. For example, Open Cloud Computing Interface (OCCI), Cloud Data Management Interface (CDMI) and Open Virtualisation Format (OVF) standards mitigate lock-in concerns [11]. In essence, one possible way businesses can reduce lock-in effect at pre-contractual phase is to at least understand the commonalities among provider interfaces, evaluate vendors/providers for cloud specific interoperability and portability standards, before choosing cloud providers.

The above suggests it is important that a reliable cloud provider is used, essentially one whose QoS guarantee (for uptime and downtime), data protection, and data retention periods is clearly reflected in contract terms. Additionally, organisations should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, and access to data by law enforcement entities (e.g. e-discovery). Since the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects. For these reasons, organisations should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the organisations' use of the

cloud, or responsibilities for infrastructure. This requires close scrutiny to the rules governing data flow within and outside the UK.

So far, concerns about contract lock-in have been a consistent theme expressed by survey respondents, in particular, concerning the treatment of data on termination. Although, contractual issues of lock-in related to termination will typically depend on whether the contract comes to a natural and expected conclusion or terminated due to the breach of contract. In either case, as stipulated in [12], the contract should make provisions for termination and the consequent handling of data. There are three key issues for businesses to consider concerning data on termination: (1) data preservation following termination – in this case firms should ensure they have reasonable time to access data, (2) data transfer – put in place, adequate tools to support transferring data or applications to a new service or back in-house, considering presently there are no legal obligation requiring cloud providers to provide data export tools, and (3) data deletion following termination – also determine how corporate data has been deleted, including the deletion of metadata and caching, seeing as 18% of businesses surveyed identified the need for data protection and metadata ownership (see Fig. 1).

V. Conclusion

In this paper we have shown that cloud computing is a venture with an attractive proposition to enterprises, small or large. Consequently, enterprises are rapidly utilising cloud technology-enabled services to address specific business needs. However, a number of challenges remain inadequately addressed and as such require close scrutiny to facilitate the widespread adoption and maturity of the cloud ecosystem. The discussions presented herein specifically address, from a business perspective, pertinent cloud computing security issues, data privacy risks, and concerns about lock-in effect at the contract level. At a higher level, this paper identifies relevant cloud-specific standards related to security, privacy, lock-in (i.e. interoperability and portability issues) as well as contractual clauses to which businesses need to exercise great attention. Considering there are many aspects to lock-in, respondents expressed their concerns highly on exit strategy and contract termination (including data retention and destruction). This also includes the importance of retaining metadata as well as data ownership rights. Moreover on the legal side, increasing attention is paid by businesses to cloud computing contracts and SLA, which are hitherto still framed in proprietary forms by cloud service providers. Further complexity to this proprietary form is that neither the terminology of SLAs nor the willingness to negotiate SLAs is consistent between different cloud providers.

To compensate for this deficiency, we provide the following strategic guidelines to aid organisations mitigate related concerns: (1) specific security-related issues can be minimised by ensuring cloud providers adhere to industry accepted cloud-specific standards, (2) cloud computing services and solutions that support standard data formats and service interfaces, facilitating interoperability and portability, must always be preferred, and (3) regarding data privacy concerns for respective businesses, a correct understanding of the responsibilities (of provider and consumer) in the processing of corporate (private) data in the cloud environment is functional to the correct allocation of legal obligations between the parties of a cloud computing service contract. Further, this is essentially important in the case of security or data privacy breach. Overall, these strategic guidelines are not meant to be exhaustive but should augment with the legal advice provided by expert lawyers when negotiating and/or drafting cloud service contracts. In summary, issues and challenges discussed may diminish as the cloud computing environment matures leading to widespread adoption, increased knowledge of use and technology acceptance. As a future work, we would like to investigate these issues further as it pertains to enterprise cloud adoption and utilisation strategies.

References

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

[2] IDC, “Cloud computing 2010 – an IDC update,” 2010. [online] Available from: http://www.cionet.com/Data/files/groups/Cloud%20Computing%202010%20-%20An%20IDC%20Update.pdf [Accessed 12th January 2015].

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

[4] Survey Monkey, “*Online Survey Development Tool*,” [online] Available from: https://www.surveymonkey.com/ [Accessed 17 September 2014].

[5] JISC Legal, "Report on Cloud Computing and the Law for UK FE and HE (An Overview)," 2011.

[6] W.K. Hon, C. Millard, and I. Walden, “Negotiating Cloud Contracts: looking At Clouds From Both Sides Now,” in 16 Stan. Tech. L. Rev. 79 2012.

[7] R. Wang, “The Enterprise Cloud Buyer’s Bill of Rights: SaaS Applications,” How to maximize your investment and avoid potential Vendor lock-in, Best Practices Report, 2012.

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

[9] ICO, "Information Commissioner’s Office. Anonymisation: managing data protection risk code of practice," ICO, November 2012.

[10] Oracle, “Architectural Strategies for Cloud Computing,” in Oracle White Paper in Enterprise Architectures, August, 2009.

[11] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap," NIST Cloud Computing Standards Working Group, Special Publication 500-291, 2011.

[12] T. Leimbach, D. Hallinan, D. Bachlechner, A. Weber, M. Jaglo, L. Hennen, R.O. Nielsen, M. Nentwich, S. StrauB, T. Lynn, and G. Hunt, "Potential and Impacts of Cloud Computing Services and Social Network Websites," Publication of Science and Technology Options Assessment, 2014.

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

[14] DPA, "Data Protection Act 1998 - Guidance on the use of cloud computing," 2012. [online] Available from: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf [Accessed 1st March 2015].

[15] Gartner, “IT Glossary: IT Industrilisation,” 2015. [online] Availiable from: http://www.gartner.com/it-glossary/it-industrialization [Accessed 13th March 2015].