

Compliance, Regulation & Legal Issues in the provision of a Secure Cloud Deployment.

Pertaining to the SME/SMB business sector

Kevin O Regan

Fortuity

kevin@fortuity.ie

086 - 3837384

***Abstract*—The SME/SMB sector is big business globally. Many of the companies in this sector are young, fast growing organizations, with very little legacy workflows that would inhibit cloud migration. As a business group they are very suitable to cloud migration. The very nature of the industry is very granular and as a result many SMB companies do not have the scales required to negotiate strongly with the far more consolidate CSP grouping. The approach for the SMB sector should not be to negotiate hard with the CSP's but to be aware of the industry standards in relation to Service level agreements, Legislation, Compliance, Regulation and Security Frameworks. Once the SMB sector has armed and familiarized itself with this information it can then analyze the market in terms of best practice and select the most suitable CSP with which to partner. This paper researches the information and approaches that the SMB sector should take in this process.**

I. INTRODUCTION

The Small to Medium size Enterprise or Small to Medium size Business sector is a huge market globally. In Europe an SMB is classified as any company with less

than 250 employees. It is estimated that the 50 million strong SMB sector globally will spend \$600 billion on IT services in 2016. SMB's are potential strong cloud adaptors as it is estimated that in excess of 30 million SMB's don't own a file server. As these organizations grow and invest in IT they are very likely to go directly to a cloud solution. It is also estimated that more than 10,000 companies each year grow beyond the upper limit of the SMB sector and leave the category [16].

Microsoft recently conducted a survey titled "Drivers and Inhibitors to Cloud Adoption for Small and Midsize Businesses". In this survey of over 3000 SMB's, the reasons that SMB's are considering the cloud are focused on financial savings, higher productivity of IT resources and greater flexibility. However, the survey also highlighted very significant concerns in relation to cloud migration. Of the 3000 companies surveyed, 70% had concerns about compliance and regulation, 52% were concerned about data privacy and data control [19]. In fact these concerns are very similar to global concerns across many industry sectors. The fact is that compliance, regulation and legal issues are restricting cloud adaption by large and small organizations alike. The very simple questions that cloud adaptors, whether large or small, are want answered are:

- Where will my data reside?

- Who will be able to see it?
- How will it be moved?

These are very basic questions that every responsible company, who is considering migrating to the cloud should consider.

But while the concerns of the SMB sector is similar to larger global players, the similarity ends there. Large enterprises have the financial leverage to be able to engage successfully with large CSP's. This makes the process somewhat easier than for the SMB sector. Unless an SMB organization is in a particular industry or sector that a CSP considers strategically aligned, the SMB does not have much bargaining power. So it is very difficult for an SMB to leverage successfully with CSP's.

The purpose of this research is to give the SMB owner a good understanding of the compliance, regulation and legal issues associated with cloud computing. By gaining a clear understanding of all the drivers and issues in this area the SMB owner can use this information to the best of his/her advantage in selecting the most suitable CSP in the market place. The SMB owner needs to understand the current & future legislation and regulation associated with key industry sectors. It is also important to understand industry standards that are being developed, legal practices that apply to different sectors and how SLA's need to be developed to protect the SMB customer and not just the interests of the CSP. Once this understanding is gained, then the cloud market place becomes easier platform to operate on and better decisions can be made in relation to selecting and managing a CSP.

II. MAIN

A. Cloud Concerns

In 2008, the then chairman of CISCO, John Chambers stated that "Cloud Computing is a security nightmare and can't be handled in traditional ways". Security issues have certainly proved to be a major inhibitor in cloud adoption since then. Cloud Security has many facets and can be broken down into three areas, technical, organizational and procedural. From an organizational and procedural viewpoint the perception is that there is a loss of control once an organizations data has been

migrated to the cloud [1]. Once data has been migrated to the cloud there is a significant dependence on a third part provider and with that come the perception that there is a lack of transparency. Also in 2008, Gartner identified that cloud computing was an area of rapid expansion, little standardization and few industry wide solutions. Control of external processes is critical and it is clear that policy and regulation are significantly behind technology [2]. Trust is a significant soft issue during the CSP selection process for all organizations and this process is mostly based on Service Level Agreements and the CSP reputation. It is clear that where ever the data is stored there will be some activity associated with this data. In addition it is also clear that CSP's have the ability to data mine. Surveys have shown that trust concerns relating to security practices, regulation and compliance have a significant impact on CSP selection. These significant barriers that have to be overcome in the selection process are all related to security, regulation & compliance

B. Service Level Agreement.(SLA)

In relation to the profile of an SMB/SME organization it is clear that unless it is in a strategically attractive industry sector it will not command much leverage when it comes to negotiations with a CSP. In addition, the CSP are typically much larger organizations and will be more interested in offering a standard solution to an SME rather than meeting the individual requirements of every SME. So the challenge for the SME owner is to identify key parameters for CSP selection. The first major item to review is the Service Level Agreement, (SLA) that is provided by the CSP. The SLA is the contract that is being offered by the CSP and is a very important legal document. It is there to protect the CSP and the customer. Key items that the SLA should include are [1], [3], [6], and [21]:

- Client has the ability to audit the CSP upon request.
- CSP needs to show compliance to standards and regulations.
- CSP needs to detail how CSP subcontractors are managed in the event of capacity overflow.
- CSP needs to detail uptime commitments.
- The SLA needs to state that all out of control incidents to be reported to client.

- The CSP should specify when and how data is duplicated or moved.
- The SLA should give full details of what logging and monitoring controls are in place.
- Incident response plans should be included.
- The client should have the right to guaranteed deletion.
- The client should understand what will happen to their data in the event of a CSP bankruptcy scenario.
- Specifications and procedures for data protection should be specified.
- The SLA should specify CSP mergers and acquisitions limitations.
- Data security and ownership should be specified.
- Data encryption requirements should be specified.
- Clear delineation of responsibilities should be documented.
- How multiple client data is segregated should be defined.
- Penalties for not meeting SLA requirements should be defined.
- Robust activity monitoring controls.

The SLA is a critical aspect in the relationship between an organization and its CSP. It should be the cornerstone on which the relationship and trust between both parties is based. As a typical SME does not have the ability to negotiate all the above items into a contract so the approach is to sample a number of SLA's from different CSP's until the most suitable partner is found based on their standard SLA.

C. Legal Requirements

Additional complexities to the compliance and regulation issues associated with cloud computing relates to the geographical spread of datacenters. Legislation regarding the storage and transportation of data across borders and continents requires very careful attention. It is very important that a global approach is taken in relation to understanding this issue. It is critical that organization have an understanding of where its data is located and how it is transported between locations. In

addition the commercial relationship between the customer the ISP and the CSP needs to be fully understood [1].

This EU Data protection act 1995 applies to data processed by automated means. The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when this processing is lawful. The legislation gives direction relating to a number of areas. Some of these focus on [9]:

- The quality of data.
- The legitimacy of data processing.
- Restrictions on how individuals may be classified.
- How the data provider is entitled to specific information from the data controller.
- How individuals have the right to object to their data being stored.
- How the requirement that any data processing be reported to a supervisory body.

One very interesting aspect of this legislation is that there is an obligation on the controller to ensure the confidentiality in the storage and processing of data. Under this legislation the client is usually the data controller and the CSP is not. Yet, it is the responsibility of the client to ensure the data is stored correctly. This requires very significant control and monitoring of CSP's be data controllers. This really is the core of the issue.

In 2012 the European Commission proposed upgrades to this legislation that have recently been passed and will become effective in 2016. These additions relate to the following areas:

- the right of the individual to be forgotten,
- that explicit and not assumed consent is required for data processing,

- An increased responsibility on the part of the data controller to report data breaches to supervisory bodies.

One very interesting point to note is that the legislation applies to data that is processed in any global location once the controller is active in the EU.

This is only a summary of the Act but it is very important that SME owners operating within the EU should understand the legislation to the point where they can utilize the legislation as part of the CSP selection process. Different global regions have varying levels of regulation and it is important that the CSP that is chosen operates in Europe to avail of the protections associated with this legislation. This is probably the single most important piece of legislation in the EU.

The USA legislation is a bit more disjointed and is covered by a number of pieces of legislation. I will details the main items in the following sections.

The Healthcare Insurance Portability and Accountability Act, (HIPPA) is US Federal legislation since 1996 and was strengthened in 2010 with the addition of the Health Information Technology for Economic and Clinical Health. (HITECH). HIPPA was created to improve the efficiency and effectiveness of health care systems in the US. HITECH extends the data privacy and security requirements of HIPPA to business associates of covered entities. This declares that CSP's who are working for HIPPA covered entities are business associates of that entity. This effectively means that these CSP's have close contractual obligations to operate in a HIPPA compliant environment. So here again, while the SME sector do not need to understand the finer details of HIPPA compliance it is worth noting that under HITECH legislation, HIPPA compliant CSP's are operating in a very controlled environment and could well offer the comfort and trust required by any SME client [7].

Sarbanes-Oxley, (SOX), regulations remains one of the biggest security drivers in publicly quoted companies. While this legislation does not pertain directly to the SME sector it is beneficial to understand the requirements and be in a position to discuss with any

potential CSP provider. SOX regulations are primarily a financial reporting mandate. There is no specific reference to technologies or security suites to be employed to achieve SOX compliance. Achieving compliance with Sarbanes-Oxley is a major driver of IT compliance and security. So any CSP that is SOX compliant will have a general high level of awareness to encryption, end point security, and intruder protection, activity monitoring and auditing controls.

The Federal Information Security Management Act, FISMA, was included as part of the USA Cyber Security Act 2012. The Act was created to improve network security within the USA Federal Government and its Contractors. This was achieved by implementing security controls and regular auditing to set standards. CSP's operating both in the EU and USA, with compliance to FISMA would be well worth considering as a CSP partner for an SME client.

Statement of Auditing Standards (SAS) No. 70 or more commonly known as SAS70 was a widely recognized standard developed by the American Institute of Certified Public Accountants. The Standard was completed on service providers. SAS70 compliant companies have completed an in-depth analysis of their controls of information technology and related topics. In 2011 SAS 70 was replaced with Statements on Standards for Attestation Engagements No 16. (SSAE 16). Today SSAE 16 is one of the most widely used standards for data centers and CSP providers. This is another standard that can be used in a questionnaire to potential CSP partners and used in determining how suitable a CSP would be for a particular SME organization.

Gramm-Leach-Bliley, (GLBA). GLBA requires financial institutions to establish standards for protecting the security and confidentiality of their client's information. In one specific technical comment the act promotes the use of encryption to protect such data. Institutions are required to provide regular statements to customers detailing how their client's data is stored and shared and how the data is protected. If financial institutions are using specific CSP's to comply with GLBA requirements then this information could help the SMB in the selection of a CSP.

D. Compliance

When dealing with compliance in regulated industry sectors there are a number of approaches that the SME sector can take. If the SME client is in a regulated environment then the client must obtain a clear understanding of the regulations associated with its sector. Whether the client is moving from an “on premise” service to a cloud service or going directly to a CSP, compliance to regulated environments is required. In other words, clients are to understand their regulatory requirements and ensure they are compliant whether they are looking at “on premise” or a cloud based solution. Alternatively, if the SME client is not in a regulated environment there are very significant benefits in understanding these regulatory requirements and selecting a CSP that is compliant in a specific regulated sector. The approach here is to understand the requirements of a regulated sector, select CSP’s that are compliant in those regulated sectors and obtain the benefits and comfort of selecting a CSP that has met the requirements of a regulated environment [13].

One of the more strictly regulated industries sectors is the Credit Card Payment Sector. The Payment Card Industry Data Security Standard, (PCI DSS). The primary focus of the standard is on minimizing the instances of credit card compromises under a number of generic headings [21]. These are –

- Build and maintain a secure network.
- Protect Card Holder Data.
- Maintain a vulnerability management program.
- Implement strong access control measurements.
- Regular monitoring of networks.
- Maintain a policy that addresses information.

PCI DSS applies to any environment where payment card data is processed, stored or transmitted. In a cloud environment the type of service provided by the CSP will have a significant bearing on the type of regulation required. In all cases a strong partnership is required between the CSP and the client to ensure the PCI DSS requirements are met. Difficulties such as the client’s lack of visibility and knowledge of the CSP infrastructure, perceived lack of control or oversight,

perception of a dynamic environment all lead to the requirement to have this strong partnership element in place. Where a CSP is promoting compliance to PCI DSS, careful evaluation of the type and nature of the compliance is required. Compliant CSP’s will be listed by payment card companies. Considerations such as how long CSP’s are compliant and when the last audit was completed are very important considerations. The overall approach for the client is to engage its technical resources to identify its needs and source a CSP that can meet those needs. But a CSP that has any level of compliance to PCI DSS should be well worth considering as a CSP for a non-regulated industry [20].

E. Security Frameworks

Another source of valuable information for SME owners considering a cloud migration process is the initiatives that CSP’s themselves have put in place in the form of security frameworks. In the following section I have given some details covering a selection of the security frameworks and organizations[22]. The main objective of these frameworks is to give support and resources to client companies from the CSP sector.

Cloud Audit A6, Automated Audit, Assertion, Assessment and Assurance. The goal of A6 is to provide a common process to allow clients that are interested in cloud services to streamline their audit process and allow CSP’s to provide a standard and secure methodology for auditing CSP’s. Cloud Audit A6 was officially launched in January 2010 and has the participation of many of the largest CSP’s

The Trusted Cloud Initiative is supported by the Cloud Security Alliance. The goal of the Trusted Cloud Initiative is to create a common service offering to meet the security needs of businesses operating in the cloud. The initiative is a methodology that enables IT professional to leverage a common set of solutions.

Common Assurance Maturity Model, CAMM is a global collaborative project with support from multinationals, professional organisations and many standards setting bodies. Its key aim is to provide a visible, and freely available standard for the transparent assurance of Services delivered by external Cloud Service Providers

COBIT is an IT framework for the governance & management of enterprise IT. COBIT incorporates enterprise governance and management techniques. It provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from information systems.

ISO/IEC 27000 is one of the best known standards body in Europe is the ISO. ISO 27000 provides best practice data and recommendations on information security and controls within the context of an overall information security management system. (ISMS) ISO 27001 is an auditable standard on Information Security Management System (ISMS) requirements. The first version of the standard was in 2005. ISO/IEC 27018 is the next ISO standard to come in stream and is focused on data protection for cloud services. ISO/IEC 27018 establishes commonly accepted control objectives and guidelines to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

The Federal Risk and Authorization Management Program, or FedRAMP, is a US government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is the result of close collaboration with cybersecurity and cloud computing professionals. FedRAMP's goal is to accelerate the adoption of secure cloud solutions through auditing & assessments.

Information Technology Infrastructure Library. ITIL advocates that IT services are aligned to the needs of the business and support its core processes. It provides guidance to organizations and individuals on how to use IT as a tool to facilitate business change, transformation and growth.

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA's activities, knowledge

and extensive network benefit the entire cloud computing industry from providers to customers.

European Union Agency for Network and Information Security, ENISA's Mission is essentially to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, and business and public sector organisations in the European Union.

All these security frameworks and organisations are a wealth of information for the SMB sector. A significant amount of information about these groups and the information they make available to commercial organisations is freely available. These organisations have a wealth of information and direction in relation to the selections of CSP's that would give a secure and regulated service to the SME sector.

III. CONCLUSIONS

The SMB sector need to select a CSP that offers a comprehensive and detailed SLA to all clients. Any SMB's that operate in a regulated environment need to ensure that they are compliant within the required regulations whether in the cloud or not. It is critical that the right relationship and open culture between the SMB client and the CSP is developed. Unregulated SMB clients can select a CSP in a regulated environment in order to take advantage of the SLA that CSP offers. For example, selecting a CSP that is proven compliant in handling credit card data should be an attractive option for most SMB clients. Legislation is developing all the time in relation to data security and the SMB sector would be well advised to remain up to date with this information. A wealth of information and advice is available from many framework and network groups in relation to Cloud Computing security.

REFERENCES

- [1] Council of Europe Professional Informatics Societies. "Cloud Computing Security & Privacy Issues" 2015
- [2] Kerr/Teng "Cloud Computing – Legal & Privacy Issues" 2012
- [3] Padhy/Patra/Satapathy "Cloud Computing Security Issues & Research Challenges" 2011
- [4] Shimba "Cloud Computing : Strategies for Cloud Computing Adaption" 2010
- [5] Alsudriari/Vasista "Cloud Computing & Privacy Regulations – An exploratory study on issues and implications" 2012
- [6] Chandra/Vaish "Privacy Issues and Measurement in Cloud Computing"
- [7] Parshant "HIPPA Compliance and Cloud Computing" 2013
- [8] NSAI "Adopting the Cloud – Decision support for Cloud Computing" 2012
- [9] Alan Harris "The legal Standing of data in a Cloud Computing Environment" 2012
- [10] Service Technology Magazine, RagYeuler "Service Security and Compliance in the Cloud" 2012
- [11] Hon/Millard/Waldron "The problem of personal data in Cloud Computing – What information is regulated ? The Cloud on knowing" 2011
- [12] ENISA – "Network & Information Security in the Finance Sector"
- [13] Ullah/Khan "Security and Privacy issues in a Cloud Computing Environment: A survey Paper" 2014
- [14] Journal of Cloud Computing "A quantitative analysis of current security concerns and solutions for Cloud Computing" 2012
- [15] Dabhi/Nouranni "Survey on Data Security Issues in Cloud Computing" 2014
- [16] Carroll/Kutze "Secure Cloud Computing – Benefits, Risks & Controls"
- [17] NIST – "Guidelines on Security & Privacy in Public Cloud Computing"
- [18] Conway/Currey "Managing Cloud Computing – A Life Cycle Approach"
- [19] Microsoft – "Drivers & Inhibitors to Cloud Computing Adoption for Small and Mid Size Businesses" 2012
- [20] Cloud Special Interest Group. PCI Security Standards Council, 2013
- [21] Blackwell/Gahan – "PCI DSS compliance – meeting the demands" 2012
- [22] Dimension Data "Securing Compliance in the public Cloud"