7-1-2013

Factors That Affect The Adoption Of Cloud Computing For An Enterprise: A Case Study Of Cloud Adoption Within Intel Corporation

Brian T. McGeogh
Intel Corporation, Leixlip, Ireland, brian.t.mcgeough@intel.com

Brian Donnellan
national university of ireland maynooth, Maynooth, Kildare, Ireland, brian.donnellan@nuim.ie

FACTORS THAT AFFECT THE ADOPTION OF CLOUD COMPUTING FOR AN ENTERPRISE: A CASE STUDY OF CLOUD ADOPTION IN INTEL CORP.

Brian McGeough, Intel Corporation, brian.mcgeough@intel.com

Brian Donnellan, National University of Ireland Maynooth, Innovation Value Institute
brian.donnellan@nuim.ie

With so much hype about cloud computing, it's easy to lose sight of why it's such an important trend. Cloud Computing (CC) has the potential to offer enterprise IT management and their employee's tremendous opportunities to solve critical challenges to better serve business. This research explores the current barriers to entries that are preventing wide scale enterprise adoption of Cloud services for critical business services and what is required to overcome such challenges and uses a case study approach to examine the actual adoption of Cloud Computing in Intel Corporation. The results of the study indicates the key factors that IT organisations and business leaders alike across an enterprise will need to consider when making Cloud Computing adoption more pervasive across their enterprise. Intel identified barriers to Cloud Adoption such as (i) the need to work closely with suppliers to commit to a timeline of when they will be in a position to support their applications in the cloud (ii) the presence of redundant configurations that are not fully proven in such highly virtual multi-tenant virtual environments that require load balanced highly available web front ends, and (iii) application security validation which is a big concern for enterprise IT organisation such as Intel in their private cloud, and (iv) having a complete understanding of application workloads and behaviours.

Keywords: *Cloud Computing, Innovation, Information and Communications Technologies and Systems, Cloud Adoption*

1 Introduction

Cloud Computing (CC) has been cited as 'the fifth utility' (along with water, electricity, gas, and telephone) whereby computing services are readily available on demand, like other utility services available in today's society (Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009). In an age of information and globalisation, massive computing power is desired to generate business insights and competitive advantage (Liu and Orban, 2010). CC is a paradigm shift in IT services delivery. This shift promises large gains in agility, efficiency and flexibility at a time when demands on data centres are growing exponentially (Iyer & Henderson, 2010). The National Institute of Standards and Technology (NIST) defines CC as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Yang & Tate, 2012). This CC model is composed of five essential characteristics**,** three service models, and four NIST deployment models that will be analysed throughout this study NIST, (2011) and each will be analysed in detail as part of the study to help identify implications for enterprise adoption. This paper provides an analysis of the successes linked to Cloud deployment in Intel Corporation to-date and the current barriers to entry that are preventing Intel and similar companies from wide scale adoption of cloud services for critical business services. The Case Study also suggests how to overcome these barriers in enabling a Cloud Environment that can transform to a dynamic scalable capability to meet future business demand. The key challenges addressed in the case study are: What are the key factors to make a successful move to CC and what are the key obstacles preventing a successful move to cloud for an enterprise? Intel identified barriers to Cloud Adoption such as (i) the need to work closely with suppliers to commit to a timeline of when they will be in a position to support their applications in the cloud (ii) the presence of redundant configurations that are not fully proven in such highly virtual multi-tenant virtual environments that require load balanced highly available web front ends, and (iii) application security validation which is a big concern for enterprise IT organisation such as Intel in their private cloud, and (iv) having a complete understanding of application workloads and behaviours.

2 Cloud Computing Adoption

2.1 IT Adoption and Diffusion

Rogers (2003) seminal work defined diffusion as the process by which "an *innovation* is *communicated* through certain *channels* over *time* among the members of a *social system*". Furthermore, he classified adopters of innovation, developed during his doctoral research and first published in the Rural Sociology journal in 1958, into five major categories; Innovators, Early Adopters, Early Majority, Late Majority and Laggards. It is important to note that, as pointed out in the work, the term "laggard" is used as a classification and not pejoratively. In a review of the prolific growth in innovation literature, Wolfe (1994) concluded that it had made little contribution to the understanding of innovative behaviour in organisations and his evaluation of the results as being "inconclusive, inconsistent and characterized by low levels of explanation" was surely an indictment of the field. Moreover, he identified three streams of research that should branch from the swelling river of innovation studies: (i) Diffusion of Innovation (DI): focused on the diffusion of an innovation over time and/or space, (ii) Organisational Innovativeness (OI): addressing the determinants of the innovativeness of organisation and (iii) Process Theory (PT): focused on the process of innovation within an organisation. A later but similar interjection by Swanson (1994) argued that current innovation theory had done little to explain IS innovation and where it stood within the general debate on organisational innovation. To address this situation he posited the following three types of IS innovation to provide a new theoretical impetus - Type I : innovations confined to the IS task, Type II: innovations supporting administration of the business and Type III : innovations imbedded in the core technology of the business. A subsequent empirical testing of the model resulted in "cautious optimism" but suggested a need for further theoretical work to refine, elaborate and extend the system (Grover et al. 1997). The implications for the emerging areas of self-service business on this typology of

innovation types will be discussed later. In a more recent and influential paper, Swanson and Ramiller (2004) start by defining IT innovation as the process by which "IT comes to be applied in novel ways" and conclude that the literature on bandwagon phenomena indicate that much supposedly innovative behaviour is actually "me too" activities . In his study we will see that Intel sees Cloud Adoption as residing within Swanson's "Type III" typology : i.e. innovations imbedded in the core technology of the business.

2.2 Cloud Adoption and Diffusion

If you consider some of the benefits of CC in terms of scalability, mobility, access, and ease of deployments, it becomes apparent the standard processes that come out of the box are not tailored for all organisations IDC, (2011). It is important to remember the processes are simply guidelines. Companies need to spend time identifying the particular needs of the organisation and developing a clear method for each unique end user to yield the best possible results in the cloud. To fully leverage cloud capabilities, enterprises need to make sure there is a solid vision, and with that, research would suggest that cloud's full potential will exceed IT expectations eventually (Harms & Yamartino, 2010). Cloud critics believe handing data to a third party with unknown levels of control just won't work. The truth lies somewhere between the two extremes and it depends on a variety of factors (Yang & Tate, 2009). Understanding when it makes sense to move data or systems to the public cloud or off premises starts with understanding what the cloud actually is. The cloud is not so much a new technology as a new way of managing technology and applications and data that reside on it. From a security perspective, IT professionals making decisions need to accurately assess whether the enterprise can truly secure data or infrastructure better than a potential cloud provider can (Harms & Yamartino, 2010). The reality is moving enterprise email systems to the cloud makes a lot of sense for certain cases. For example, smaller enterprises often lack the expertise in IT and security to manage Microsoft Exchange. Likewise, when you look at infrastructure providers such as Amazon, Rackspace or Google, it is hard to say a small or even midsized organisation will do a better job securing cloud infrastructures. Cost savings are also gained in several other areas, including IT equipment, labour and data centre real estate, not to mention power and cooling savings (Iyer & Henderson, 2010). CC demands a deep understanding of business needs coupled with multi-domain expertise that allow companies to design, build and operate highly efficient IT infrastructures that include legacy infrastructures aligned tightly with business priorities (Yang & Tate, 2009). Existing business behaviours and processes will not change just because IT infrastructures do. Implementing cloud infrastructures inside your companies firewall, (Private Cloud) demands a thorough evaluation of the impact on both people and relevant business processes, and can be a difficult lesson to learn. What gets lost is the right service centric IT strategy that ensures alignment of IT decisions with business priorities (Kertesz et al, 2009). Cloud infrastructures must seamlessly integrate with the existing environment as well as leverage rigorous automation to drive value into the enterprise.

2.3 Security Risks

Software Development teams today when adopting a CC SaaS or PaaS development strategy now focus on functionality. They rely on some of the better known PaaS offerings such as Amazon BeanStalk, Microsoft Azure and Salesforce Heroku to manage the infrastructure and data management. But, as with all things Cloud, PaaS does offer some security concerns because many of the underlying security features are outside of the customer's control (Heiser & Cearley, 2011). There is also a wide variety of data encryption mechanisms are of relatively greater interest in a multi-tenanted cloud service than within the physically and logically controlled enterprise (Harms & Yamartino, 2010). The Cloud Security Alliance, an international organisation with both end-user and vendor participation, represents the most active effort on the part of IT and security specialists to improve the state of the art of CC risk management. They offer a wide range of committees working on multiple aspects of CC security. First published in late 2009, with a third version scheduled for the end of 2011, the CSA document "Security Guidance for Critical Areas of Focus in CC" is arguably the definitive framework of risk issues that need to be specifically addressed in the CC context, NIST, (2010). The NIST, in 2011, published a draft Information Processing Standard Publication, SP 800-46, "Security Guidance for Critical Areas of Focus in CC." The NIST material is intended to will guide federal, state and local government practices in the

U.S. and will be considered as sources of best practices by many governments and private enterprises around the globe. The introduction of standards for cloud security practice and assessment represents the most significant development in dealing with concerns about cloud security NIST, (2012).

2.4 Data Risks

The strategy of developing applications on the cloud is not without risks. A concern many CIO's are faced with is all it takes is one major incident of losing confidential information on the cloud for adoption rates to slow down. Current legislation related to data transfer across geographical boundaries also creates impediments. In the case of the EU, current privacy laws place rigid limits on the free flow of personal information beyond the jurisdiction of users. Similarly, in the financial services industry, audit requirements mandate that companies know where their information resides when it is transmitted, impeding cloud adoption (Iyer, 2011). In moving to the Cloud it is important business requirements are understood and the cloud service is selected to meet these needs. Iyer says: "Taking a good governance approach, such as COBIT, is an important step to safely embracing the cloud and its benefits" (Iyer, 2011). Since IT is not managing the complete technology stack in the cloud, they need to be more concerned now than ever on how to maintain compliance with corporate, legal, or government regulations. While it's true that part of the stack is in the cloud, remember that you are still running your own applications. The cloud provider is responsible for the security of the hypervisor and below, while the customer's responsibility begins at the operating system level and above. Compliance in the cloud is really not that much different from traditional on-premises technologies where processes are subject to regulation and you must ensure you use the right tools and processes (Chow, et al, 2009). If you properly deploy the tools and processes needed to secure your applications and data, you can successfully meet your compliance requirements in the cloud. For example, the Sarbanes-Oxley Act (SOX) requires strict controls over financial data. A service provider needs to provide very fine grained controls and options to govern who can access what object under which conditions. In turn, customers must use that access control to make sure they comply with SOX.

2.5 Cloud Dependability

Building a dependable cloud is an aspirational concept that can be best described as cloud service that has availability, security, scalability, risk management, i.e. all attributes necessary to host Enterprise applications, but can be provided consistently and at a reasonable price. Enterprise consumers of Cloud are looking to land apps externally to cloud faster than many have expected, but are doing so in fear and trepidation (Reeves, 2011). This is mainly due to the lack of consistency; standards and cost structures that are needed to enable the wide scale adoption and deliver to the overall promise of Cloud. Enterprise consumers today are mostly targeting non-business critical low risk applications with little governance or business process controls in place and are being forced down this path due to cost (Yang & Tate, 2012). The problem facing most Enterprises is the current state of CC is not deemed dependable enough for the large enterprise or mission critical applications (Iyer & Henderson, 2010). The demand from enterprise to move toward a more dependable cloud services, so if services do not mature based on the enterprise demand, there is a real threat that their market will dry up so more emphasis is required to create Enterprise Clouds (Reeves, 2011).

2.6 Enterprise Cloud Maturity

The Open Data Centre Alliance (ODCA) is an independent organisation of leading global enterprise and service provider IT managers and leaders who have come together to amplify their collective voice to set data centre requirements for today and the future. Their mission focuses on delivering next generation data centre and cloud solutions to meet the challenges facing IT in an open, industry standard and multi-vendor fashion. Enterprises such as Intel are working collaboratively with global IT leaders, with enterprise and service providers towards these goals and serves as an advisor to the Open Data Centre Alliance. Intel serves as a non-voting, technical advisor to the organisation. Figure 1 is a maturity model that has been published by the ODCA to drive the industry to meet the demand for enterprise adoption for

all IT services. The maturity profile maps out the specific steps needed to ultimately deliver a federated and open cloud maturity that delivers to the overall dependable vision.

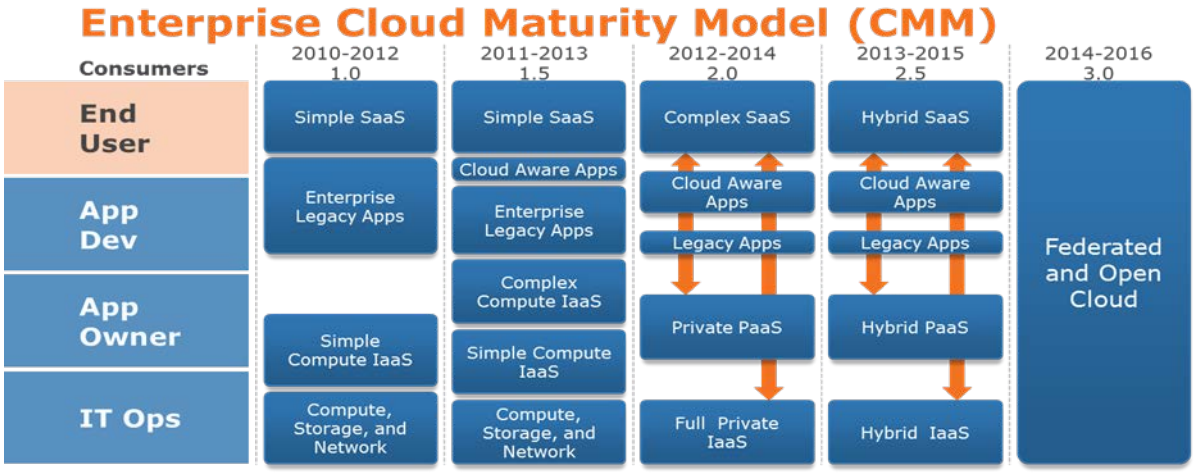

Figure 1 ODCA Enterprise Cloud Maturity Model (ODCA 2012)

As Enterprises begin to progress with the adoption cloud services, consumers and providers need to figure out how to the maturity of their cloud offering using a series of instruments to measure the risk areas of availability, security, and interoperability; along with agreed liability. Consumers of Cloud will not be able to place critical apps in the cloud unless they have a clear understanding of liability and on the contrary, providers will also find it difficult to assume all liability (Reeves, 2011). Multi-tenancy incurs more liability than the value of the provider and insurance premiums can make the support model too risky for providers and cloud break cloud model. Another concern is with chained liability where a service is dependent on multiple providers, where it would be even more difficult to understand who has the ultimate responsibility for a service outage or data loss (Harms & Yamartino, 2010). Compared to grid computing, Cloud offers two main features that drive this rapid adoption; first, Cloud offers virtualization and thus immediate access of resources; second, through hiding deployment details, Cloud offers an easier entry point for users than the rather complex and management-intensive grid computing environments (Vaquero et al. 2009, Marston et al. 2011). Since Cloud adoption is a rather novel field of study, there are only few papers dealing with this topic mostly focusing on cloud adoption in a business context. For instance, (Low et al, 2011) identify factors that affect the adoption of cloud models by firms belonging to the high-tech industry analyses the effects of institutional influences on an enterprises intention to adopt Cloud and investigates the impact of cloud adoption on IT effectiveness (Saya et al. 2010; Chebrolu, 2011). Yang concluded that practitioner and academic interest in the evolving phenomenon of CC is intense (Yang & Tate, 2009). Cloud services providers do not offer extensive guarantees or remedy many of the security and regulatory requirements of enterprise IT customers (Harms & Yamartino, 2010). As this level of automation is still evolving and IP protection relating back to security is the need to protect core intellectual property, a company's "crown jewels", is of paramount importance to enterprise IT teams. The lack of interoperability causes a fear of vendor lock in and for cloud to be truly realised to provide for more automation, shared and dynamic resources and federation of multiple cloud environments together in a seamless way requires interoperability and standards based hardware and software (Yang & Tate, 2009). From a related study by (Zarnekow et al, 2012), the barriers for the adoption of CC are identified as the lack of standards and appropriate selection requirements (Leavitt, 2009; Clemons and Chen, 2011). Furthermore, many offers do not meet or only partially meet customer requirements. The absence of defined Cloud requirements and evaluation criteria makes it difficult for customers to plan migration projects and implement sustainable Cloud solutions. The fact that interoperability between providers hasn't been achieved makes a provider selection often irreversible or requires much effort (Hoefer and Karagiannis, 2010; Repschlaeger and Zarnekow, 2011). This difficulty, known as "provider lock-in", is discussed extensively and is an important topic for practitioners and for several initiatives, e.g. the Open Grid Forum (OGF) or the Distributed Management Task Force (DMTF) (Cattedu and Hogben, 2009; Armbrust et al., 2009; Ortiz, 2011).

3 Research Method

A number of authors have provided guidance on the conduct of high quality interpretative research (e.g. Miles & Huberman (1994); Klein and Myers, 1999; McKay & Marshall, 2000) and case studies, in particular (e.g. Yin, 1984; Walsham, 1995; Darke et al., 1998). For example, Darke et al. (1998) address five specific difficulties: selecting appropriate research, designing, shaping, and scoping a case study research project, obtaining the participation of organisations, collecting case study data from case participants and establishing rigour in writing up case study research. In contrast, Carroll & Swatman (2000), provide a framework to assist in undertaking and assessing the theory building aspects of interpretive Information Services research. Yin (1984), describes a protocol for case studies, which, as he suggests, "contains the instrument but also contains the procedures and the general rules that should be followed in using the instrument." Greenhalgh (1997) has proposed nine questions for evaluating papers that describe qualitative research in general based on her own research and from the research of Denzin and Lincoln (1994), Mays and Pope (1996) and Britten et al (1995). Since this research seeks to answer "how" and exploratory "what" questions on an emerging phenomenon, qualitative case study methodology was selected (Benbasat et al, 1987, Eisenhardt 1989, Yin 2003). Furthermore, because of the position and context of the research in the Intel Corporation feel that the case is ideal for revelatory cases where an observer may have access to a phenomenon that was previously inaccessible (Yin 1984). The reason why a Case study was selected for this study was it excels at bringing an understanding of a complex issue or object and can extend experience or add strength to what is already known through previous research (Flyvbjerg, 2011). Case studies emphasise detailed contextual analysis of a limited number of events or conditions and their relationships. Yin defines the case study research method as an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used (Yin, 1984). Through the work of researchers such as Benbasat et al. (1987) and Yin (1984) case studies, particularly those designed to be consistent with positivist criteria, are accepted as a legitimate and useful method of IS research (Klein and Myers, 1999). Their purpose is to try to understand, interpret, phenomena in terms of the subjective meanings people bring to them (Denzin, 1994). However, as Walsham (1995) suggests "the most appropriate method for conducting empirical research in the interpretative tradition is the in-depth case study". There are important factors and considerations for the decision to adopt CC and the current studies and research in this field can be summarised to focus around the questions why adoption of CC would occur, how much adoption would take place or how it would be adopted (Luoma and Nyberg, 2011, Nuseibeh, 2011). As case studies can be complex and involve multiple sources of data, which can include multiple cases within a study, and produce large amounts of data for analysis. The advantages of the case study method are its applicability to real-life, contemporary, human situations and its public accessibility through written reports. Case study results relate directly to the everyday experience and facilitate an understanding of complex real-life situations (Soy, 1997). The research for this study used a combination of quantitative and qualitative research methods into the challenges related to measure the level of cloud adoption within an enterprise utilising frameworks such as the Innovation Value Institute (IVI) IT Capability Maturity Framework (IT CMF) to provide the quantitative measures applying a design science research approach. The IT CMF was complimented by qualitative measures through a series of semi structured interviews from both IT and business experts within Intel IT to validate assessment findings to assess the level of adoption within the enterprise and what key factors to drive more pervasive adoption. The study answers research questions identifying the current limitations and makes recommendations as to what improvements can be applied to the overall assessment process and make recommendation implement. The reasons for using the IT-CMF in this case were twofold: (i) the practice-led resarch environment in which the framework was developed. Since its inception in 2006, the IT-CMF has been used by a variety of global organizations to solve a range of capability issues - IT capability measurement and improvement, IT organizational design and capability management, IT business alignment and leadership, Organization benchmarking and best practice and IT risk management. IVI represents 'triple-helix' support and innovation across academia, government and industry. The approach has been to determine the current maturity of both an organization's cloud computing capabilities and its risk management capabilities. As such, the Cloud Computing tool and the Risk Management (RM) Critical Capability of the IT Capability

Maturity Framework (IT-CMF) are effective maturity assessment instruments to enable organizations to establish future roadmaps that will improve their maturity with respect to their cloud computing readiness. Increasing the level of maturity improves organizational practices surrounding the identification and mitigation of risks/threats that pertain to the cloud environment. The IT Capability Maturity Frameworks assessments providing the initial data analysis followed by semi structured interviews that provided additional qualitative data. The author collected the opinions of thought leaders in the field of Cloud in order to understand their views on opportunities, threats and trends which CC presents. There are various forms of interview design that can be developed to obtain thick, rich data utilizing a qualitative investigational perspective (Creswell, 2007). Taking a semi-structured interview approach provided the necessary flexibility allowing a better flow of responses during the interview. By probing into the details of the assessment results, the Author was able to get more depth on the topics being discussed. The informal conversational interview is outlined for the purpose of relying "entirely on the spontaneous generation of questions in a natural interaction, typically one that occurs as part of on-going participant observation fieldwork". As McNamara (2009) stated, the strength of the general interview guide approach is the ability of the researcher" to ensure that the same general areas of information are collected from each interviewee. This provides more focus than the conversational approach, but still allows a degree of freedom and adaptability in getting the information from the interviewee". Participants were asked identical questions, but the questions are worded so that responses were open-ended. This open-endedness allows the participants to contribute as much detailed information as they desire and it also allows the researcher to ask probing questions as a means of follow-up. The interviewer in this semi-structured interview approach provided the interviewee with a series of five questions to focus on the issues being explored. The participants involved in the research were senior technology personnel as part of a Intel's Cloud Program Team offering a range of CC services (Infrastructure, Platform and Software) which provided a good coverage to the overall subject area being researched. From the literature review it was clear that the complexity of CC meant there were more than technology issues at play in deciding how to build CC in to business and IT strategies. The primary research took a balanced approach combining the applying the Innovation Value Institutes (IVI) IT Capability Maturity Framework (CMF) Cloud Assessment methodology along with a series of questions to compliment the assessments and provide a more holistic view of the key factors of Cloud adoption.

4 The Case Study: The Adoption of Cloud Computing in Intel Corp

Participants were asked identical questions, but the questions are worded so that responses were open-ended. This open-endedness allows the participants to contribute as much detailed information as they desire and it also allows the researcher to ask probing questions as a means of follow-up. The primary research took a balanced approach combining the applying the Innovation Value Institutes (IVI) IT Capability Maturity Framework (CMF) Cloud Assessment methodology. Complimented with a series of questions to increase the relevance of the study by providing a more holistic view of the key factors of Cloud adoption. Through this semi-structured interview process the author developed an interview strategy by identifying themes based on the research questions focusing on the views from both IT and the Business contacts. The body of knowledge assembled in previous stages of the work was used to craft a suitable question to elicit pertinent information on the drivers, benefits and challenges of CC. As CC is an emerging technology, it necessitated a level of exploratory questioning to gain a better understanding of the core concepts of the paradigm, enabling the interview process to address specific themes while having the flexibility to alter some of the themes and questions as dictated by the flow of questioning. Saunders deems this valuable given the specific organisational context that is encountered in relation to the topic being researched (Saunders et al., 2003). For the promised ROI from cloud services to be realised, the impact it will have throughout the enterprise and how it will impact the ability to operate the business, service customers, innovate, and even adopt other technologies in the future. Ultimately, IT and the technologies IT deploys are now, more than ever, direct contributors to business success. This, in turn, leads to the need and resources for continued investments in the latest technologies and services that can be delivered more efficiently from the cloud. It's a vicious cycle that will provide a return on investment for a business well beyond what any ROI calculator may say. It is now up to each individual enterprise to determine when and how they want to leverage all that cloud has to offer and to find the best cloud partner to help them achieve and accelerate the real business benefits of cloud. The CMF Cloud

Assessment Processes assesses an Enterprise IT capability maturity to position, evaluate, introduce and manage cloud services. It has a management life cycle from cloud adoption readiness to on-going management of the cloud environment, covering strategic positioning, business benefits and financial model, Governance including compliance and reporting, Implications for Enterprise Architecture (EA), sourcing selection, solution delivery Service provisioning, on-going supplier management and risk management and compliance. Initial observation from the Intel IT CMF maturity assessment results is that they score on average 2.90 ranging from 2.6 – 3.3, so overall an intermediate level of maturity. This in high level terms translates that the strategy of moving to the cloud and how it progresses the business objectives has been defined. Intelligence has been gathered on cloud service offerings and providers. There is an understanding of what strategic requirements will be satisfied by using the available cloud service offerings and providers. Results would indicate that they have a very clear business and IT strategy - High ratings across these critical processes, ITG, BP and SP (Architect); also highlighting good day to day management of the environment - High SD (Manage). The Intel Cloud appears to fulfil many of the key enterprise user requirements – SRP (Design), SRC (Negotiate) and SD (Manage). Suppliers are well managed – High SRC (Manage). The key areas the interviews focused on were the top and bottom scores as the outliers, as the majority of the other scores were within an average maturity threshold of 2.9 illustrating an overall intermediate level of cloud maturity. The scores that came in lowest were all in relation to sourcing (SRC) of cloud capabilities across three of the four SRC sections of the lifecycle (identify, supply chain and review). It was also interesting to see that the highest score is also linked to sourcing, the only SRC capability (negotiate) not called out in the low scores SRC scores, to overall ranging from 1.0 to 4.0. During the interviews the Author used the standard open ended questions to better understand the reasons behind the high and low scored and this was a key focus area.

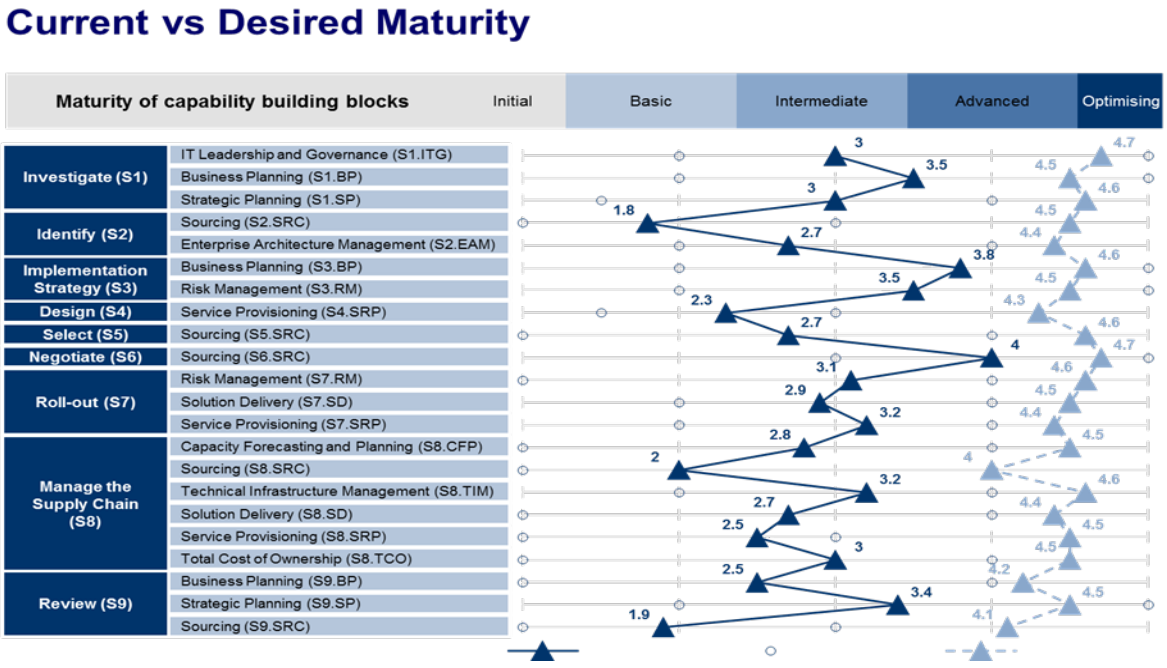

Figure 2 Intel Current vs. Desired Maturity results.

4.1 Maturity Model Analysis

Some of the key areas for discussion during the interviews was to understand the relational linked to the low scores with identification and selection of new suppliers; Low SRC (Identification, Select and Review) and poor capacity planning and forecasting; Low CFP (Manage) Difficulty with the integration of existing services with new cloud services; Low EAM (Design) and TIM (Manage). The enterprise appears to be struggling with the holistic implementation of cloud services; Low SD (Roll-out) and SRP (Roll-out). From the assessment results, there were two key points that needed to be addressed. Although the day to day management of the business is doing well, they are struggling to implement new

services, so there was a need to determine if this is for all new services or just for Cloud based services. Some CC's score differently depending on where they were used in the Life Cycle. For example SRC had low scores for Identification Select and Review, but high scores for Negotiate and Manage. This implies that the organisation is struggling to identify and introduce new service providers, but is quite good at managing and working with existing providers. Further assessment concluded that here is that the procurement process within Intel is very robust, but the focus put on the application of cloud sourcing needs to be improved. The study also analysed the future desired maturity, these results were also quite interesting. Overall *Maturity Desired: 4.46 (4.0 – 4.7) Min 4.0 Max 4.7;* and I would question is this a realistic goal to achieve, so during the SME interview, the author also probed into the reason behind the responses and tried to gain a better understanding for why this group was scoring the future state at such a high level of maturity; mainly due to high expectations of the Intel team to achieve very high maturity in the near future as they see this as a competitive advantage for their business. It was also assessed that the areas that were scored lowest in the current maturity state also mapped to the future state with SRC (identify, supply chain and review). There were also some lower scores that also seemed to be and SRC (negotiate) one of the highest in the desired maturity. Also interesting and not surprising, as Intel have a very strong procurement process, so most assessed would agree they need to improve the maturity of how they apply sourcing and procurement within their cloud supply chain.

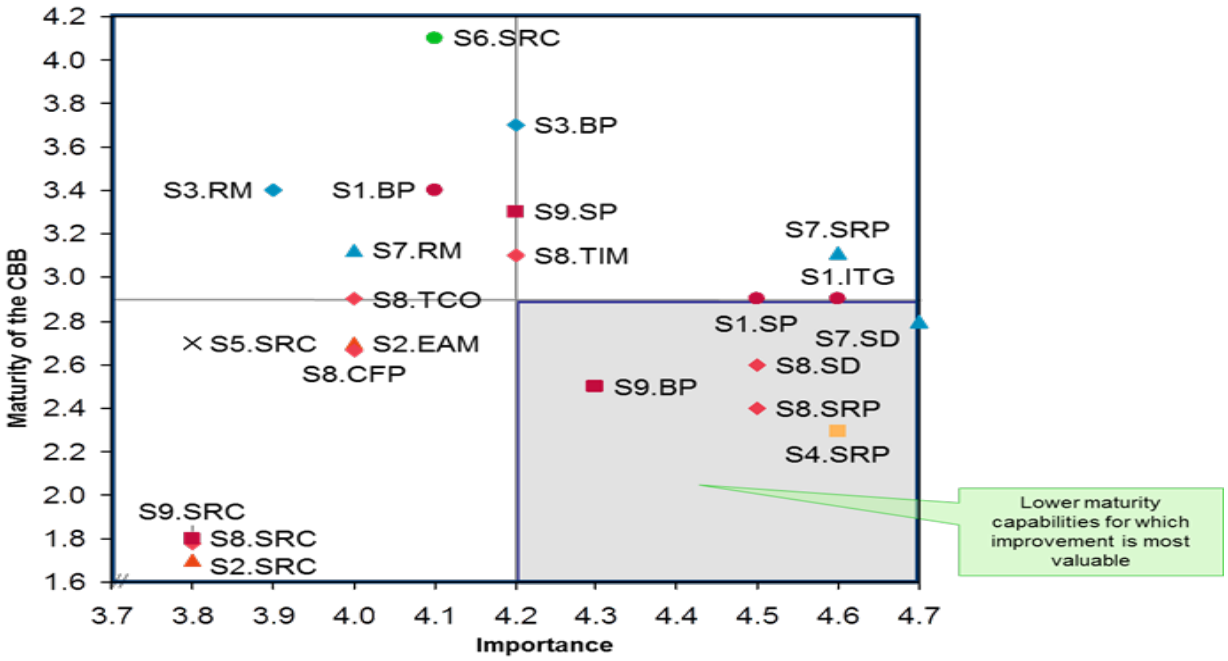

Figure 3 Intel Cloud Adoption Maturity Results: Importance vs. Maturity

In Figure 3, this four quadrant diagram graphically maps each of the maturity levels of the Capability Building Blocks (CBB) with the level of importance as scored in the current state assessment. The results from the Intel's assessment highlights BP (investigate), SD (rollout and supply chain), SRP (design and supply chain) and SP (Investigate) are all of high importance and low maturity. Observations from these results highlight some interesting challenges for Intel IT. As there may need to be trade-offs as to where they start to focus their priorities. During the SME interviews the Author was able help analyse the assessment findings and correlate the data to better provide Intel with more meaningful information to help them decide what CBB or lifecycle phase should be prioritised and this will be discussed in the next section. It was evident that all interviewees unanimously agreed that the Intel IT business drivers for cloud across Business and IT are linked to agility, availability, efficiency, and security. Enabling strategies include: End-to-end on-demand self-service capabilities; End-to-end health/performance monitoring and action integrated operational data analytics and trouble-shooting. Intel IT need to go ahead and break old enterprise applications and replace them with new cloud-enabled solutions. Also, they need innovation in security solutions that enables IT to protect data and services. Having business processes in place that is leveraging the management capabilities compute, storage, and network and

facility integration was essential. They should consider the key attributes of the cloud services must deliver accessibility, required features, reliability, and cost for the business to be willing to consume these services. Success to date have been linked to the emphasis on having organisational commitment within IT with strong CIO and Staff level support/directives along with Business level agreement to drive and adopt cloud and be recognised by all as a strategic enabler for the enterprise.

4.2 Factors that affect Cloud Adoption in Intel

4.2.1 Technical Factors

Enterprises like Intel need to work closely with suppliers to commit to a timeline of when they will be in a position to support their applications in the cloud. Until such a time, their hands are tied and will need to support these apps in a physical infrastructure. Some issues are also linked to Real Time Applications not able to be virtualized due to the architecture of the application as they are relegated to physical hardware; so no real solutions targeted here and most likely these apps will remain outside the cloud. The industry is starting to see progress in the maturity level of the vendor offerings to allow solutions in the near term are of enterprise mission critical applications. As applications typically have complex redundant configurations that are not fully proven in such highly virtual multi-tenant virtual environments that require load balanced highly available web front ends (eg. Network Load Balancing Software and Big IP hardware load balancing for secure networks). Application Security validation spans all aspects of cloud and is a big concern for enterprise IT organisation such as Intel in their private cloud, and having a complete understandings of application workloads and behaviours in critical. Hypervisor security (i.e. inability to determine if it has been compromised), also requires the use of new technology solutions to ensure VM's are valid. The good news is that most of these technical limiters do not appear to be insurmountable, but until resolved, do dull benefits of cloud capabilities to many of its most critical business applications. The industry needs to push suppliers of these capabilities to ensure roadmaps are in place to address these technical limiters and are hopeful that they will deliver solutions to mitigate these issues in the near future. Effective cloud security revolves around the right mix of security tools and technologies. The list might include intrusion detection; web filtering, malware protection, encryption and data loss prevention. Yet it also requires well-conceived security policies that match the enterprise requirements and direct employees appropriately. Compliance and regulatory issues also factor into the equation, with the ability to manage and restrict data is critical and with the open nature of clouds makes this task more challenging. Consequently, companies must introduce policies, practices and protections that mesh with increasingly onerous and complex regulatory requirements in some cases spanning countries.

4.2.2 Non-Technical Factors

While there are many benefits for a enterprise consumers to adopt some of the services offered by cloud service provider, the applicability of these services will depend on the nature and size of the enterprise, not all services are applicable for a particular enterprise. In addition, the applicability of a particular service for a particular enterprise will also depend on the size of an organization. For instance, a particular service may be applicable for an enterprise when that enterprise is in start-up stage. As the enterprise grows its business, the same service which was applicable earlier, may seize to be so when the enterprise becomes big. Factors like economies of scale will play a major role in determining the economic viability of a particular service to the enterprise, Infosys Technologies, (2009). While security is clearly a primary concern for most enterprise IT consumers, this research would support that those who have already deployed cloud services, often in the form of private clouds, generally feel confident in their abilities to manage security in the cloud. The strategic value of CC is compelling enough that companies are still moving forward despite concerns about protecting data and infrastructure and reports of high-profile attacks in the news. The assessment findings report that for the majority, security issues are a significant factor in the decision to deploy a private versus public cloud in some cases the foundation of that decision. This reinforces other industry studies that have shown that the journey to the cloud often starts with a private delivery model typically because of security concerns. While security challenges are many, the results indicate that they can be overcome by a solid investment in security controls, including solutions that protect data and data centre infrastructure from attacks top security drivers for those

surveyed. As enterprises are making substantial investments in cloud security to protect assets, thwart infrastructure attacks, and meet compliance requirements. The IT professionals who took part in these surveys are managing security challenges by prioritising security as part of their cloud planning, conducting in-depth research, and leveraging or establishing strong vendor relationships. The good news is that as IT professionals move through the planning, evaluation, and implementation stages, they gain valuable knowledge and experience with security that really pays off in the final deployment. As several of the interview respondents recommended, when it comes to cloud security, "do your homework." Those surveyed were well aware that threat activity is increasing and cyber criminals are continuing to develop more sophisticated methods of attack. Efforts to expose these will be on going even as cloud services delivery models continue to evolve. The challenge for the IT industry is to continue to adapt so that enterprises can continue to maintain or even increase confidence in the security of their assets.

5 Summary and Conclusions

Cloud promises to provide better performance, reliability and scalability (Erdogmus, 2009). There is some evidence that these are being delivered, (Fox et al., 2009). All in all, these promises have drawn increasing attention at a world wide scale. This research explores the current barriers to entries that are preventing wide scale enterprise adoption of Cloud services for critical business services and what is required to overcome such challenges and uses a case study approach to examine the actual adoption of Cloud Computing in Intel Corporation. The results of the study indicates the key factors that IT organisations and business leaders alike across an enterprise will need to consider when making Cloud Computing adoption more pervasive across their enterprise. Intel identified barriers to Cloud Adoption such as (i) the need to work closely with suppliers to commit to a timeline of when they will be in a position to support their applications in the cloud (ii) the presence of redundant configurations that are not fully proven in such highly virtual multi-tenant virtual environments that require load balanced highly available web front ends, and (iii) application security validation which is a big concern for enterprise IT organisation such as Intel in their private cloud, and (iv) having a complete understanding of application workloads and behaviours. The findings of this case study indicate that experienced IT professionals most often would encourage others to be thorough in their CC planning and to continuously prioritise security any have them engaged from the very beginning of any future cloud initiatives. The research suggests that IT managers should focus much attention on developing their cloud strategy and to take a cautious approach when deploying mission critical application into the cloud. Any enterprise cloud implementation must allow for continuous processing of transactions that enable business success, regardless of where your systems, applications or data reside. Business resiliency should be an inherent attribute within the fabric of the cloud design and as such, needs to be part of your critical design efforts. What this study uncovered is a new concept coined as around "Dependable Cloud", which is an effort to better define what Enterprise IT must do to confront issues mainly with security and privacy, performance and service level agreements, define who controls information, and how to best deliver services, all while managing practical and cultural changes.

6 References

A Alter, A. E., Peng, Y., Runhua, L. and Harris, J. G. (2010). China's Pragmatic Path to Cloud Computing. Accenture Research Report

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010). A view of cloud computing. Communications of the ACM.

Badger et al, (2011) Government Cloud Computing Technology Roadmap, [Online] Available from: http://www.nist.gov/itl/cloud [Accessed 20 June 2012]

Bernius & Kroenung, (2012), Fostering Academic Research by Cloud Computing – The Users' Perspective, Goethe University Frankfurt, Grueneburgplatz, IT Global Services and Cloud Computing.

Brown, G. (2008). Who invented the term cloud computing?. [Online] Available from: http://groups.google.com/group/cloudcomputing/ [Accessed 20 June 2012]

Cachin, Keidar, and Shraer, (2009). Trusting the cloud. SIGACT News 40, 2.
Carr, N. (2003). "IT Doesn't Matter." Harvard Business Review 81 (5): 41-49.
Carcary, M. (2006). Ex-Post evaluation and review of the implementation of a student Management Information; System (MIS) at Limerick Institute of Technology: a case study.
Cassidy, A., (2009) Cloud Computing; what is in it for us? Dissertation submitted to the University of Dublin.
Chow, et al, (2009). Controlling data in the cloud: outsourcing computation without outsourcing control.
Cohen, R. (2008). Who invented the term cloud computing?, [Online] Available from: http://www.elasticvapor.com/2008_12_01_archive.html [Accessed 20 May 2012]
Curley, M, (2006) Transforming Intel IT: The Intel IT Business Plan, MIS Quarterly Executive Vol. 5 No. 4 / 155
Curley, Martin.,(2004) Managing Information Technology for Business Value". Intel Press
Gartner (2009). Gartner Identifies the Top 10 Strategic Technologies for 2010. Gartner Press Release.
Grover, V., Fiedler, K., and Teng, J. (1997). "Empirical Evidence on Swanson's Tri-Core Model of Information Systems Innovation." *Information Systems Research*, 8(3), 273-287.
Harms & Yamartino (2010). The Economics of the Cloud: Microsoft.
Heiser & Cearley (2011) Hype Cycle for Cloud Security, Source: Gartner
Holden & Lynch (2004) Choosing the Appropriate Methodology: Understanding Research Philosophy.
IDC (2009). IT Cloud Services Forecast: 2009-2013. IDC announcement.
Intel Press, (2011) Cloud Security Insights for IT Strategic Planning, Intel IT Centre.
Iyer, B. and J. Henderson, (2010). Preparing for the Future: Understanding the Seven Capabilities of Cloud Computing. MIS Quarterly Executive,
Johnson, (2012) Cloud outage report of 13 providers reveals downtime costs, http://go.techtarget.com
Kertesz, Kecskemeti, and Brandic. (2009). An SLA-based resource virtualization approach for on-demand service provision. In Proceedings of the 3rd international workshop on Virtualization technologies in distributed.
Li, H., Sedayao, J., Hahn-Steichen, J., Jimison, E., Spence, C, and Chahal, S. (2009). Cloud Developing an Enterprise Cloud Computing Strategy. [Online] Available from: http://www.intel.com/au/directions/pdf/Cloud_Computing_Strategy.pdf
Lu Liu, (2012) Dependable Service-Oriented and Cloud computing, IEEE HPCC 2012.
Masser, P.,Tjoa, and Huemer (2009). "Retaining Data Control to the Client in Infrastructure Clouds," Availability, Reliability and Security.
McGeough et al, (2011), Best Practices for Building an Enterprise Private Cloud: Intel Press.
Myers, M. D. (1997). Qualitative Research in Information Systems, *MIS Quarterly* (21:2), June 1997, pp. 241-242. *MISQ Discovery*.
ODCA (2012) Open Data Center Alliance: http://www.opendatacenteralliance.org/
Reeves, (2011), The Dependable Cloud and Hybrid IT, Dependable Cloud Conference.
Rogers, E. M. (2003). *Diffusion of Innovations (fifth edition)*, Free Press, New York.
Saunders, M., Lewis, P. and Thornhill, A. (2003), Research Methods for Business
Soy, Susan K. (1997). The case study as a research method. Unpublished paper, university of Texas at Austin.
Swanson, E. B. (1994). "Information Systems Innovation among Organisations." *Management Science*, 40(9), 1069-1092.
Swanson, E. B., and Ramiller, N. C. (2004). "Innovating Mindfully with Information Technology." *MIS Quarterly* 28(4), 553-583
West, D., (2010) Saving Money Through Cloud Computing, The Brookings Institution: Washington DC.
Vaquero, L.M., Rodero-Merino, L., Caceres, J., and Lindner, M.(2009) A Break in the Clouds: Towards a Cloud Definition, ACM SIGCOMM Computer Communication Review
Yang & Tate, (2009), Where are we at with Cloud Computing?: A Descriptive Literature Review, 20th Australasian Conference on Information Systems; 2-4 Dec 2009;
Wolfe, R. A. (1994). "Organizational Innovation: Review, Critique and Suggested Research Directions." *Journal of Management Studies* 31(3), 405-431.
Zarnekow et all, (2012) Cloud Requirements Framework: Requirements and Evaluation Criteria to Adopt Cloud Solutions, Technical University of Berlin, IT Global Services and Cloud Computing