Gordon Institute
of Business Science
University of Pretoria

Cloud Computing in a South African Bank

Name: Arno van der Merwe

Student number: 91159190

Contact details: 082 418 1732, arnom@absa.co.za

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

11 November 2013

Abstract

This research looked at cloud computing in a South African bank. Interviews were conducted in the information technology sector of a major bank in South Arica, as part of a deductive research method, to establish how cloud computing should be understood, what are specific benefits, obstacles, risks and if the benefits outweigh the obstacles and risks.

The research demonstrated that cloud computing is a fairly new concept in South African banks especially when it comes to the public cloud. Private clouds are currently in existence, especially in the form of data centres and virtualised services. The research also indicated that benefits outweigh obstacles and risks, with cost seen as the most important benefit in contrast to privacy and security as the most important obstacle to consider.

It would be difficult for a bank in South Africa to move into the public cloud and the focus would be to move no-core services into a public cloud and to keep the core services within the bank.

It should be noted that the research sample was limited to only one of the major banks in South African and that it would be inaccurate to present the results as a complete view of banks in South Africa.

Keywords

Cloud computing

South African bank

Information technology

Declaration

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

Name: Signature:

                               Date:

Acknowledgements

I would like to thank the following people who supported me through this journey:

My supervisor, Roy for his guidance and patience.

My employer who made this possible by giving me the time needed to complete the research.

Anneke Booyens, a dear friend who supported me on a continuous basis.

My parents for their support in difficult times.

Contents

1. Introduction

Information technology (IT) expenditure in organisations worldwide for 2012 comes to around $3.6 trillion with expected growth for 2013 to be around 4.1 percent, which is nearly double the growth of 2.1 percent for 2012 (Gartner n.d.).

Gartner (n.d.) described cloud computing as a "disruptive phenomenon, with the potential to make IT organisations more responsive than ever. Cloud computing promises economic advantages, speed, agility, flexibility, infinite elasticity and innovation. How will you phase your organization into cloud computing?" This is supported by Sultan (2013) who mentioned that there has never been such a disruptive innovation in the IT space since the development of the web. Berman, Kesterson-Townes, Marshall and Srivathsa (2012) mentioned cloud as a "technology game changer because it offers anytime, anywhere services, its potential for driving business innovation remains largely untapped", supported by Gold (2012) who described cloud as a major technological trend and that businesses are faced with a decision to join the trend or not.

"The agility and cost-efficiency enabled by cloud computing has some large banks, including ING, proactively testing the technology. But other bankers are cautiously awaiting answers to security and regulatory questions. Still others aren't even quite sure what cloud computing is." (BS&T Survey: Banks Take to Cloud Computing, Banktech, 2010). Mackay, Baker and Al-Yasiri (2012) mentioned cloud computing as one of the significant features of computing in the last ten years but also stated that a number of technical barriers still exists, preventing it to be a truly open and simplified solution. Issues mentioned by Mackay et al. (2012) is data security and a lack of trust by the users that cloud should be central to their IT Infrastructure.

The question is not if businesses will move to cloud but when they move to cloud if they will be able to balance the risk and reward of cloud computing (Kalyvas, Overly & Karlyn, 2013).

The research to be conducted focused on a technology application and more specifically cloud computing in a South African (SA) bank. The review focused on cloud computing, how it developed over recent years, the specific focus areas of cloud and what key areas of old technology cloud computing can replace in an enterprise today. Specific focus was given to the success factors or benefits of cloud computing, obstacles of cloud computing, and privacy and security issues. The research specifically focused on the benefits and obstacles of cloud computing in SA banks. The scope of the research was limited to SA banks and was deductive, exploratory research in the form of unstructured and semi-structured interviews. The research was exploratory in nature by searching the academic literature, interviewing experts and conducting interviews (Saunders & Lewis, 2012). Firstly a pilot study was conducted in the form of an unstructured interview from where a final interview schedule was compiled for the semi-structured interviews.

The research objectives were as follow:
- To understand cloud computing in all it shapes and facets in a SA bank.
- To establish/understand the benefits that can flow from making use of cloud computing in a SA bank.
- To establish and understand the major obstacles or risks with the use of cloud computing in a SA bank.
- To establish if the benefits outweigh the obstacles and risks for implementing cloud computing in a SA bank.

2. Literature review

2.1 Cloud computing: history and definition

The term cloud computing was used as early as 1997 and has only recently become a more regularly used term (Lin & Chen, 2012). Several definitions were found in the literature and it seems that the cloud computing morphed from Software as a Service (SaaS), as early definitions referred to cloud computing as being the "delivery of IT and business functionality in a utility environment" Guptil and Mcnee (2008), or a "long held dream of computing as utility" (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, & Zaharia, 2010). Business functionality has always been offered as a service but the core change/improvement with SaaS was the move to multi-tenant architecture explained Guptill and Mcnee (2008).

The next move is then the move into the cloud and Hayes (2008) took it further to call it "on demand computing supported by (Mishra, Jain and Duressi, 2012), SaaS or Internet as the platform" and that the key shift is the change of geography of computing. Tucker, as cited in Greeger (2009) defined cloud as the "...movement of applications services onto the Internet and the increased use of the Internet to access a wide variety of services, traditionally originating from a company's data center", also supported by Chin-Nung, I-Liang and Yan-Kai (2011) and Greenguard (2010) with additional comments of a quick and affordable way to use IT Infrastructure services as Internet service. Brynjolfsson, Hofmann and Jordan (2010) even went one step further by mentioning cloud as a catalyst for innovation as long as it becomes more affordable and more omnipresent.

Cusumano (2010) explained cloud as an industry platform which will become the new platforms for enterprise and personal computing replacing traditional software running directly on desktops and handheld devices. Complete elimination though will not happen any time soon as delivery will require a significant rewriting of code to cater for all the interfaces and services. Von Solms and Vijoen (2011) defined cloud computing

3

as a "computing model which allows one to access an IT service over a network, as or when it is needed, without worrying about the technical details of how the service is provided," and Lin and Chen (2012) added a pool of resources, hardware and software, which is easy to access through the Internet. Rader (2012) added a business flavour and described cloud as "conducting business functions on shared, off-premises computing systems", which offer strategic options but also some business control challenges for the organisation. Sood (2012) referred to cloud computing as the saving of user data on an off-site storage system which is then maintained by a service provider.

Mell and Grance as cited in Garrison, Kim and Wakefield (2012) came up with a consolidated definition: "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of resources (such as networks, servers, storage, applications and services) that can be quickly provisioned and released with minimal effort or service provider interaction."

2.2 Service models of cloud computing

Literature is split on the service models for cloud computing with SaaS being mentioned as one of the first service models and Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) added later (Durkee, 2010; Garrison et al. 2012; Lin & Chen, 2012).

Srivastava and Kumar (2011) discussed these service models in more detail as the architectural layers of cloud computing:

SaaS - a complete application offered as a service on demand, thus a single instance of software runs on cloud and services more than one end user.

Paas – this service encapsulates a layer of software and provides it as a service that can be used to build higher level of services. This can be looked at from two perspectives, either providing middleware, application software and a development

environment, all as one service, or an encapsulated service through an Application Program Interface (API). In the case of the API the platform manage and scale resources to provide a certain required level of service.

IaaS – this is the provision of basic storage and compute capabilities as a service over a network, thus servers, storage systems, switches and routers together with other systems are pooled and made available to handle workloads. The range can be from application components to high performance computing applications.

Garrison et al. (2012) discussed these service models briefly:
SaaS – access to software hosted through a thin client by the cloud vendor, where the vendor has complete control over the application which includes capabilities, updates and maintenance of the application.

PaaS – a model in which the cloud vendor provides the platform for creation and deployment of applications and service which is then accessed by the organisation through the Web/Internet.

IaaS – servers, storage and connectivity provided by the cloud vendor and the client being charged based on usage.

Lin and Chen (2012) mentioned four service models with "Service" being added together with SaaS. They described SaaS and Service as one concept with the idea of being subscription by customers to applications or services to free up their own IT resources.

2.3 Delivery/Deployment models for cloud computing

Deployment models of cloud computing, or in some literature called delivery models, are Public cloud, Private cloud and Hybrid cloud Garrison et al. (2012). Another model added by von Solms and Viljoen (2011) is known as Community cloud.

Certain characteristics of these models mentioned by von Solms and Viljoen (2011) and Srivastava and Kumar (2011) are as follow:

Public cloud

- IT resources owned and managed by a third party and accessible to the general public or a large industry over the internet
- Situated or hosted away from the organisations' premises.
- Provides the lowest level of direct control, but provides a flexible extension of the organisations' infrastructure.
- Leads to reduction of start up costs and frees up resources so that focus can be on IT solutions for real business problems

Private cloud

- IT resources are virtualised, thus the resources are available as a pool that can quickly be provisioned on demand in any single organisation
- Cloud belongs to one organisation, thus they own the infrastructure and how the applications are deployed.
- High level of control is achieved and governance is easier for e.g. security and quality of service.
- The organisation implements and maintains the cloud.
- Either in the form of a data center or collocation facility.

Hybrid cloud

- Two or more models of cloud are linked to enable data or application portability for e.g. applications exist in the public cloud and data exist in the private cloud, especially when data is classified as sensitive.
- Supplement resources of the private cloud with resources in the public cloud in times of extensive workloads so that service levels are maintained.

- Public cloud can be used to handle work spikes by performing certain periodic tasks
- Complexity in a hybrid cloud around the distribution of applications across the public and private cloud.

Community cloud
- Normally supports a community of users/organisations
- Cloud can be managed by the organisation themselves or through a third party.

2.4 Benefits/Value and Issues/Concerns with cloud computing

Three distinct aspects of cloud computing are mentioned by Ambrust et al. (2010) in comparison with traditional computing and are the following,
- Infinite resources are available on demand
- Elimination of upfront commitment by cloud users as you can start out small and increase hardware resources as required.
- The ability to use computing resources on a short term basis when you need the resources and release the resources when they are no longer required.

Ambrust et al. (2010) then listed ten obstacles and opportunities for potential growth of cloud computing.

	Obstacle	Opportunity
1	Availability/ Business Continuity	Use multiple cloud providers
2	Data Lock-In	Standardise on API's
3	Data Confidentiality and Auditability	Deploy encryption, virtual local area network (VLAN) and firewalls
4	Data transfer bottlenecks	FedExing Disks and higher bandwidth switches

5	Performance unpredictability	Improve Virtual Machine (VM) Support, Flash memory and Gang Schedule VM's
6	Scalable storage- not a given	Invent Scalable Store
7	Bugs in large distributed systems	Invent Debugger that relies on distributed VM's
8	Scaling quickly – to save money and resources	Invent Auto- scaler that relies on machine learning (ML): Snapshots for conservation
9	Reputation Fate Sharing	Offer reputation guarding services like those in place for email
10	Software Licensing	Offer Pay for use licensing

Ambrust et al. (2010) predicted that it should be taken into account by the developers that cloud would grow and came to conclusion that application software needs to scale down and up rapidly and a pay for use licensing model is required. Infrastructure software needs to adapt from bare metal to being run on virtual machines. Metering and billing should be in place from the start. Hardware systems should be designed at scale, such that cost of operations matches the performance and the cost of purchase equally.

Cusumano (2010) acknowledged many advantages and disadvantages with cloud computing. Key for Cusumano (2010) for the future of cloud computing and coexistence of multiple platforms is that vendors should maintain some sort of differentiation among their platform offerings, direct platforms are not too powerful and switching should be easy and inexpensive for both user and developer.

Durkee (2010) mentioned specific needs to be addressed such as unused capacity in large corporate data centers and the development of "highly capable Internet data communications infrastructure. Durkee (2010) highlighted economies of scale by delivering of computing, via a centralised, shared infrastructure and that this has set an expectation of lower cost through cloud than traditional in-house computing. He goes so far as to predict that cloud will become a commodity as a result of lower prices and

perfect competition. Perfect competition is when many providers deliver the same service or product in a highly price competitive environment.

Some challenges highlighted by Durkee (2010) is based on technical and organisational challenges and that these need to be overcome to ensure large scale adoption of cloud computing. Essential characteristics mentioned by Durkee (2010) are the following:

- On demand access – the rapid fulfilment of demand for computing and the ability to deliver continuously.
- Elasticity – computing provided as requested and easy to dispose if no longer required also supported by Zhang, Li and Zheng (2011) when they mentioned cloud computing as a flexible and cheap way for deployment of IT infrastructure in an elastic way.
- Pay per use – utility based and charged on quantity used.
- Connectivity – all servers to be connected to a high speed network that allows proper flow of data to the Internet and between computing and storage.
- Resource pooling – the provider infrastructure should be shared across customers to achieve economies of scale at computing and service layers.
- Abstracted Infrastructure – end user or the customer does not always know the exact location or type of infrastructure that the applications are running on. Thus performance metrics should be in place to guarantee a minimum performance level.
- Little or no commitment – this might interfere with the services demanded by the organisation and traditional Service Level Agreements (SLA's) have to be adopted.

Durkee (2010) then placed the focus on the cloud service provider and mentioned that as a result of perfect competition the service provider tend to avoid this situation by:

- Differentiating the product though advertising instead of true and unique characteristics
- Obscuring pricing through hidden fees

- Make product information difficult to understand so that they have the control over the information
- Cutting corners and poor product quality to enhance profits
- Try to lock customers into long term commitments without delivering clear benefits.

Cloud providers are also unsure or unclear on specifics of the underlying hardware and software stacks that are required to deliver virtual servers to the end user or customer. This sometimes result in over-commitment and specific techniques for over commitment as mentioned by Durkee (2010) are:

- Specific memory allocation and leave CPU unspecified
- Quote shared resources to the maximum, instead of specific allocation for the customer
- Offer a range of performance for a certain instance
- Over-allocate resources or also known as "thin provisioning" can also lead to reduced performance during peak times

Some other strategies from cloud providers to achieve lower pricing are traffic shaping, using older gigabit of fast Ethernet, recycling failed disk drives, deployment of older disk drives, deployment of older central processing unit (CPU) technology and long term commitments to overcome lower margins (Durkee, 2010).

Durkee (2010) mentioned concepts such as Cloud 1.0 and Cloud 2.0. With Cloud 1.0 the expectation is that the customer is required to understand the trade-offs made by the supplier/vendor to offer the services at a low price. In the cloud space SLA's are not always on the order of the day, performance is never discussed and more people in the organisation becomes responsible for production computing without any system administration background. This then creates the opportunity for the cloud service provider to provide offerings around housekeeping and support (Durkee, 2010).

Cloud 2.0 will focus on solutions rather than computing cycles only and the key is to look at the cost of downtime and what is mission critical for the organisation stated Durkee (2010). Challenges for cloud 2.0 will be the following to provide storage on par with in-house especially with regards to reliability and performance.

Benefits of cloud 2.0 will be:
- High service levels
- Problems and solutions to be methodical and not random
- Infrastructure to scale automatically
- Automatic disaster recovery
- Minimise staffing and less power usage

Durkee (2010) came to the conclusion that two transformations are required for cloud: Firstly, provide value to the organisation so that they will move from their own purpose built data centers and proprietary IT departments. Secondly, provide fast and reliable cloud computing with necessary service and support required by the end user.

Greengard (2010) mentioned specific challenges such as the lack of connectivity and adequate bandwidth, especially in environment where dial up networks persist to exist. Another problem is the dependability of local power supply which can lead to inaccessibility to data or data being lost in the cloud. Mobile technology as platform will be important in cases where power supply becomes a problem, as mobile technology can be extended to remote areas especially where traditional networks do not exist (Greengard, 2010).

Ryan (2011) pointed out some privacy concerns with cloud computing through an example of a cloud based conference management system. These issues are universal to other cloud systems and are accidental or deliberate disclosure of data and that cloud computing in general allows aggregation of data which then creates opportunities for abuse especially when in the wrong hands. Ryan (2011) also explained that clear policies should be in place for usage of data in the cloud. A proposal by Ryan (2011) is

the appointment of data custodians who do not manipulate or distribute the data for e.g. Google, with legislation in place to protect data, as there is already legislation in place to protect personal data. The question then remains how one protects data in the cloud where the data resides on servers.

Srivastava and Kumar (2011) mentioned three aspects in cloud:
- The illusion of infinite computing resources available, thus no planning required for provisioning
- No large capital expenditure to start and can increase hardware resources as required
- Te ability to pay for the service as required based on usage, on short demand and the release of the service when no longer required

Also mentioned by Srivastava and Kumar (2011) are new application opportunities such as mobile interactive applications, parallel batch processing (100 computers for a short time instead of few for a long time), analytics (for decision making), and the extension of compute intensive desktop applications.

Srivastava and Kumar (2011) mentioned that cloud architecture address some important difficulties with large scale traditional data processing. Some of these difficulties are:
- With traditional data processing it is difficult to get as many machines as the application needs
- It is difficult to get the machines when they are needed
- It is difficult to distribute and coordinate large scale jobs on different machines, run the process and then provision other machines for recovery
- It is difficult to scale up or down based on active workloads
- It is difficult to dispose of machines when the work is completed

Srivastava and Kumar (2011) propose an on demand, self service, pay by use model. The environment needs to be elastic by expanding and contracting based on demand or

workload. Pay by use may take the nature of leases with minimum level of support from the cloud provider. Virtualisation is key for this model as it allows organisations to quickly create copies of current environments, involving multiple virtual machines to support, test, develop and stage activities. Cost should be minimal as the environments can coexist on the same servers used for production and fewer resources are used. The risk shifts from the organisation to the cloud provider for procurement of infrastructure (Srivastava & Kumar 2011).

Considerations to move from standard enterprise application deployment to one based on cloud explained Srivastava and Kumar (2011), should be to look at the specific deployment models and the complementary benefits of these, the service models and open API's vs. Proprietary API's.

Lin and Chen (2012) specifically looked at the factors that influence the rate of cloud adoption by business, how cloud is perceived by IT professionals and concerns these professionals have with regard to adoption of cloud. The theory used was based on "diffusion on innovation" to help them identify factors encouraging and preventing adoption. Potential benefits mentioned by Lin and Chen (2012) are from a financial and resources perspective:

- Reduction in capital expenditure and the running and maintaining of the hardware
- Universal access to software and services reduce the need for software licenses and reduce costs
- Elasticity, due to resource management being more flexible
- With PaaS you get an agile development environment for quick application development and instant adoption with no more waiting for hardware and software implementation

Some obstacles mentioned by Lin and Chen (2012) are:
- Lack of constant high speed Internet connection as cloud relies on the Internet for service delivery

13

- Lack of standardisation of API's and platform technologies results in poor integration between platforms and makes transfer or switching difficult between cloud providers
- Lack of control and loss of control which results in security and privacy issues especially data privacy and data confidentiality, thus who controls the data in the cloud

Four categories of risks for using cloud are mentioned by Lin and Chen (2012) are policy and organisational risk, technical risk, legal risk and risk not specific to cloud but to the infrastructure it relies on for e.g. networks. Other issues are also the availability and reliability of the service and can be disrupted by downtime which in turn leads to increased project or business/operations risk, explained Lin and Chen (2012).

2.5 Summary of literature

The literature reviewed came to a comprehensible conclusion of what cloud computing is, the service models were identified and deployment or delivery models were explained. It was however not clear from the literature what service models and deployment models will suit what type of organisation or industry.

Opportunities or potential opportunities for growth of cloud computing was mentioned and were linked to specific obstacles to overcome. Specific obstacles and how to overcome these were mentioned by Ambrust et al. (2010) but these were again generalised and not specific to an organisation or industry.

Some literature focused on the disadvantages or obstacles with cloud computing, especially Durkee (2010), mentioned the fact of cloud becoming a commodity and the perfect competition amongst cloud service providers. Durkee (2010) also mentioned some obstacles that needed to be overcome and although different wording is used, it more or less aligned to Ambrust et al. (2010). For example. Durkee (2010) mentioned on demand access where Ambrust et al. (2010) mentioned availability or business

continuity. These are in principle the same. Another example is where Ambrust et al. (2010) mentioned performance unpredictability and Durkee (2010) mentioned abstracted infrastructure which also speaks to performance and the measurement thereof.

One distinct difference is that Durkee (2010) also focused on the cloud service provider and what expectations could be required from the cloud provider to overcome some of its obstacles. Durkee (2010) warned against over-commitment by cloud providers and the ever present drive to provide services at a lower price which may impact the service to the customer.

As can be seen from the literature, benefits, opportunities, obstacles and disadvantages are converged. It is thus not clear which are true benefits and how hard the organisation will have to work to convert opportunities into clear and concise benefits. It is also not clear what are true obstacles and disadvantages for specific organisations and how they can overcome these. Clear categories however emerged from the literature reviewed and are identified as resources, solutions, performance and reliability, cost, service provider, privacy and security, and risks and this will be used as main headings to categorise the benefits, opportunities, obstacles and disadvantages.

A consolidated summary from the literature of specific benefits or opportunities of cloud computing are provided below and categorised as follow to provide clarity. Privacy and risks as categories are excluded.

Resources
- Elasticity
- Minimise of staffing and less power usage (electricity usage)

Solutions
- Problems and solutions to be methodical and not random
- Infrastructure to scale automatically

- Automatic disaster recovery
- Quick application development and adoption through PaaS .
- Application opportunities as mentioned such as:
    - Mobile interactive applications
    - Parallel batch processing
    - Analytics
    - Extension of compute extensive desktop applications

Cost
- Elasticity
- Reduction in capital expenditure or layout
- Reduction in the running/support and maintenance of the infrastructure
- Universal access to software and services which will reduce the need for software licenses and the related costs

Service provider
- High service levels – with cloud 2.0 as defined by Durkee (2010)

Consolidated obstacles or disadvantages with cloud computing as identified from the literature reviewed are categorised as follow to provide clarity. The only difference is that solutions as category are replaced with performance and reliability.

Resources
- The adaptability to scale quickly
- Scalable storage is not a given
- The illusion of infinite computing resources being available

Performance and reliability
- Availability/Business continuity
- Permance is unpredictable

- Bottlenecks with data transfer
- Bugs in the cloud
- Lack of constant high speed Internet

Cost

- The adaptability to scale quickly
- Scalable storage is not a given
- No large capital expenditure required – is this really the case?
- Pay for service as needed and on usage base and easy to dispose or release when no longer required – is this really the case?

Service provider

- Perfect competition from a cloud service provider perspective
- The expectation of low cost with cloud services and the related conduct by the cloud service provider.

Privacy and security

- Privacy concerns – accidental or deliberate disclosure of data and how does one protect data in the cloud.
- Lack of control and loss of control which links to security and privacy issues – who controls the data in the cloud?

Risks

- Policy and organisation risk
- Technical risk
- Legal risk
- Risk associated with the infrastructure for e.g. the network
- Business and operational risk.

The specific research objective flow from the literature reviewed and will focus on the benefits and obstacles of cloud computing exclusively in a banking environment and if the benefits for a bank outweigh the obstacles and risks.

3. Research objectives and questions

The research objectives are:

- To understand cloud computing in all it shapes and facets in a SA bank.
- To establish/understand the benefits that can flow from making use of cloud computing in a SA bank.
- To establish and understand the major obstacles or risks with the use of cloud computing in a SA bank.
- To establish if the benefits outweigh the obstacles and risks for implementing cloud computing in a SA bank.

The research questions to be answered will be:

1. How should cloud be understood in a SA banking environment?
2. What are the benefits of cloud computing in a SA bank?
3. What are the obstacles and risks of cloud computing in a SA bank?
4. Do the benefits outweigh the issues and risks for cloud computing in a bank in SA?

4. Research methodology

4.1 Design

The approach to the research conducted relied on deduction which is defined as a research approach that "involves testing of theoretical propositions by using a research strategy designed to perform this test" (Saunders and Lewis, 2012, p. 108). Research questions were defined from the existing theory.

The research study was exploratory in nature where the aim of the research was "to seek new insight, ask new questions and to assess topics in a new light" (Saunders and Lewis, 2012, p. 110). The research relied on interviews being conducted in line with the literature reviewed and data collected was analysed qualitatively and quantitatively.

The universe or population for this study was South African banks. The scope of the research was limited to the literature reviewed and the specific research objectives. The sampling frame for the data collected was all South African banks, or the "complete list" (Saunders and Lewis, 2012, p. 133) of all banks in South Africa that are classified as banks in South Africa.

4.2 Sampling method

The sample, which can be defined as "a subgroup of the whole population" (Saunders and Lewis, 2012, p.132), consisted of a subset of the SA banks and was a purposive sample. This means that sample was selected according to the researcher's judgement "based on a range of possible reasons and premises" (Saunders and Lewis, 2012, p. 138). The purposive sample was homogenous in nature which means that it consisted of one subgroup. This subgroup was one of the major banks and focused on a homogeneous group within the bank, more specifically employees in the Information Technology (IT) sector of the bank. The led to minimum variation for specific data collected. This group of people are close to the world of cloud computing and provided

the researcher with in depth answers for questions and opinions asked, especially around key themes or characteristics as pre-defined from the literature reviewed.

4.3 Data collection

Data collection was conducted using unstructured and semi-structured interviews, where the interviewer have clear ideas about the topics to explore (Saunders and Lewis, 2012). Here the focus was to use the key themes or categories from the literature reviewed and ask general questions around these key themes. An interview schedule (Appendix 1) was developed specifically around the research questions being asked.

The pilot study relied on an unstructured interview which is defined by Saunders and Lewis (2012) as a method of data collection where the participant talks openly about the topic with little intervention from the interviewer, although the focus with the pilot interview was to test the pre-defined interview questions and identify potential issues with forthcoming interviews such as time constraints, recording etc.

An adjustment was made to question one of the interview schedule as the question seemed to be too open-ended. Question one was therefore divided into three categories to enable the researcher to collect more appropriate data. Question five was also amended and instead of five top benefits and obstacles/risks interviewees were only asked for three of each. The rating of question five was also discarded as not all interviewees rated the benefits and obstacles/risks.

After the pilot interview the focus moved to semi-structured interviews, where predetermined questions were asked to participants. The order of the questions might however be varied and some topics might be excluded and additional questions be asked (Saunders and Lewis, 2012), which were applied in certain cases where interviewees were unclear about a question or asked that the researcher come back to the question later on in the interview.

21

Eight interviews in total (including the pilot interview) were conducted as part of a non-probability sample. The interviews including the pilot interview targeted people in the researchers' workplace/organisation, which is one of the major banks in South Africa. Specific sectors targeted in the workplace were the IT sector, with specific focus in the IT Infrastructure and Digital sectors. An expert on cloud computing in SA banks, from a well known consulting firm, was also interviewed.

Specific job roles of interviewees in the organisation where interviews were conducted:
- Interviewee 1: Group Technology Infrastructure Services: Chief Operating Officer (GTIS COO)
- Interviewee 2: Group Technology Infrastructure Services Co-Head (GTIS: Co-Head)
- Interviewee 3: Group Technology Infrastructure Services Head of Engineering (GTIS: Head of Engineering)
- Interviewee 4: Group Technology Infrastructure Services Specialist Engineering (GTIS: Specialist Engineering)
- Interviewee 5: Group Technology Infrastructure Services Manager Mobile (GTIS: Manager Mobile)
- Interviewee 6: Senior Manager: Technology (Expert from consulting firm)
- Interviewee 7: Group Technology Infrastructure Services Co-Head (GTIS: Co-Head)
- Interviewee 8: Head of Technology Retail and Business Banking (RBB) and Digital (Head Technology: RBB and Digital)

4.4 Analysis approach

The data collected through the interviews were analysed as qualitative and quantitative data. Questions one, five and six were analysed as qualitative data only, with question two, three and four being analysed as both qualitative and quantitative. The data was recorded on paper in the form of notes taken during the interviews, with audio recordings as back-up. The analysis was manual by default. Quantitative data was

specifically identified as categorical ranked data as a result of a ranking scale that was used to rank data from interviewees from most important, important, some importance and not important. The quantitative data is presented in graphs and tables and more specifically bar graphs to indicate the values for each specific category/ranking. This ensured that the highest and lowest values are clear for each variable under the specific category for e.g. benefits, obstacles and risks.

The analysis of the qualitative data was deductive where the researcher looked for specific themes in the data to answer the research questions as developed from the literature reviewed. Patton (2002) mentioned that qualitative data analysis is the transformation of data into findings, without a specific formula and that the final destination is unique for each one and known only when arrived at. The categories were developed from the literature reviewed and the specific research questions were based on these with specific focus on a SA bank. Units of data for the qualitative analysis are sentences and responses from the interview schedules. These sentences and responses were separately tabled/accounted for as part of each question where qualitative data was collected.

The data collected was categorised according to the literature and specific research questions asked originally. Other categories were created where emergent patterns or new themes in the data had been identified from the interview notes.

4.5 Research limitations

The following limitations have been identified:
1. The sample was limited to one major bank in SA, more specifically the IT sector in the organisation.
2. Only one person was interviewed as part of the pilot or initial study.
3. It was difficult to get time allocated from the potential interviewee's.

5. Results

Eight people were interviewed, seven from a major bank and specifically individuals that work in the IT sector of the organisation. Specific areas in the IT sector included IT Infrastructure and IT Digital. An expert on cloud computing in SA banks was also interviewed.

Notes were made for each interview conducted and data was analysed as qualitative and quantitative data. A deductive approach was applied for qualitative data where categories were established from the literature reviewed so that the research questions could be answered.

Analysis was performed by making use of interview notes and categorising the sentences or responses under the relevant categories by making use of tables. Quantitative data was collected as part of the interviews, specifically for questions two, three and four. This data was collected through a rating scale and are summarised in tables and graphs as categorical ranked data.

Question 1: How should cloud computing be understood or defined, especially in the South African banking environment.

Interviewee 1 – Pilot (GTIS COO)

Pooled resource and used by multiple.

Cloud should be guided by regulation.

Protection of Private Information (POPI) – currently a bill and will become an act once ratified.

What can be processed via cloud infrastructure and still maintain confidentiality?

Service models are dependent on regulation of financial institution.

Chinese wall – investment banking term for ring fenced environment.

Private cloud is most relevant in a bank environment.

Interviewee 2 (GTIS Co-Head)

General

Minimise cost of software and hardware as you will utilise as service.

Pay per use model will reduce maintenance.

Banks can focus on their core business.

Service models

SaaS – specialised, can possibly work for e.g. HR which is no-core.

IaaS – Data Centres run at very high facility cost especially cooling and power. This can potentially move to a service provider, with some long term cost benefits.

Important is encryption of data while in transit and also where it will be stored (location).

Deployment models

Public cloud not for SA banks currently. The time is right to explore for non-critical for e.g. email – 200MB internal vs. 10 GIG on GMAIL.

Private cloud, SA banks have these for some time for e.g. storage and virtualisation.

Cloud offering should be sharing with other banks, currently legacy software is a huge hindrance.

Interviewee 3 (GTIS Head of Engineering)

General

Cloud computing is new for banks in SA.

Service models

SaaS and PaaS: models for the development and UAT environments, but not in a production environment.

Charges based on usage and share environments with multiple customers.

Deployment models

Public – access to all, Private – internal

Hybrid – combination and best fit for the organisation. Security and risks issues to be considered

Cloud is out there – sharing of resources, virtualisation and outsource, with pay per resource usage for e.g. Kalahari.com and Amazon.

Interviewee 4 (Specialist Engineering)

General

Cloud is a simple concept, why do I need to own infrastructure (support and maintenance)?

Secure with service provider – best of practise.

It is about agility- the service provider to provide the infrastructure services in the cloud in hours – time to execution speed.

Financial services in South Africa have three to four main competitors and current bottle neck is speed.

Thus cloud is an enabler of speed (time to market).

Some information security issues, thus financial services industry is a slow adopter of cloud as result.

Sensitive information exists in financial services industry.

Service models

Huge spend on Infrastructure, thus move to IaaS. Infrastructure layer should be in place, standardised and transparent.

PaaS- maybe more relevant, the IP resides in applications – the services and products the bank provides. Competitive advantage and uniqueness of products and services.

SaaS – some models are in that space

Deployment models

Financial services industry will at first deploy a private model. Sensitivity, privacy and governance around these deployment models to be resolved first.

Then a hybrid should follow as next model and later on full public cloud deployment model.

Interviewee 5 (Manager: Mobile)

General

Cloud is a pooled resource, will only use software etc. when needed and only gets billed for the usage.

This should lead to savings on software licenses, as an example.

Service models

All service models will be relevant in a bank environment.

Deployment models

Hybrid model for the bank as some clients do make use of our systems already. Some information is used by clients/suppliers. Some confidential information required to be kept in the bank, for example intellectual property (IP).

Interviewee 6 (Expert)

General

Cloud is not a new technology, rather a new way of delivering IT services and resources.

Service models

IaaS – this model is very relevant and bottom of the stack. To be used for development and testing – thus about agility and should be in public space. Example is Amazon as service provider for Dutch banks from global perspective.

PaaS – this model is about innovation for banks, the creation and development of new services by using development tools. It is dependent on customer demands and quick deployment of these services.

SaaS – a model for non- core applications in bank and not for core applications. Examples exist where banks use for collaboration, human resources (HR), email, customer relationship management (CRM) (Common Wealth bank in Australia). Use technology to get to the customer, thus about the relationship.

Deployment models

Depends – core banking will be private cloud solutions, thus not shared and control stays within the bank.

Public cloud – capital layout is less, non-core bank applications – not in SA as yet.

Five criteria for public – multi-tenant in nature, control is limited, self-service (can scale up or down), pay-per-use and over broad band network.

Hybrid – use public cloud for e.g. at month end (trend going forward)

Community cloud – group/organisations that have a shared interest, result is economies of scale. The cost is lower than private cloud.

Interviewee 7 (GTIS CO-Head)

General

Cloud is an open ended definition; it depends on how one defines.

Environment where resources are shared for e.g. infrastructure and applications, provisioning is quickly, re- used and shared.

Mainframe is already cloud, package in such a way by the supplier.

Service Models

SaaS – Long term the way to go for e.g. HR and payroll for smaller organisations. Scale already exists in larger organisations such as banks. Exchange (email) is still a control/risk issue in the bank environment.

PaaS – back to scale and only a life cycle management benefit.

IaaS- if you can get the service form the original equipment manufacturer (OEM) for example, advanced interactive executive (AIX), the hardware and software becomes very cheap and provides lock-in forma supplier perspective. Some supplier risks – what if "fly by night''. It has to be win-win for supplier and client.

Is data centres core business for a bank and should they own these?

IT should however be core business for a bank, as it is key for the bank to survive.

Deployment models

Public – banks in SA cannot consider right now, Protection of Personal Information (POPI). The control perspective is not the same with public cloud.

Internal and external cloud: The control issues lies with external cloud for the bank environment.

Interviewee 8 (Head of Technology: RBB and Digital)

General

Key is security, customer privacy- these are the biggest hurdles for cloud computing in banks.

Security- sign up cloud provider and indemnify for potential security breaches.

Scale, speed to market, capital investment

Public cloud – this is not for a bank

Private – a definite yes for a bank

Also decide if it will be a virtual cloud or not.

Non- banking activities (non- core) can be in the public cloud, no spill over from core to non- core to occur.

Cloud is the provisioning of capability without investment in capital expenditure/services. One can rent the cloud or subscribe to a service for e.g. account opening on cheque accounts.

Service models

Data is the problem, especially in public cloud.

Deployment models

Public – this model not for SA bank. Security and Privacy is still an issue, bank might lose their license or be sanctioned.

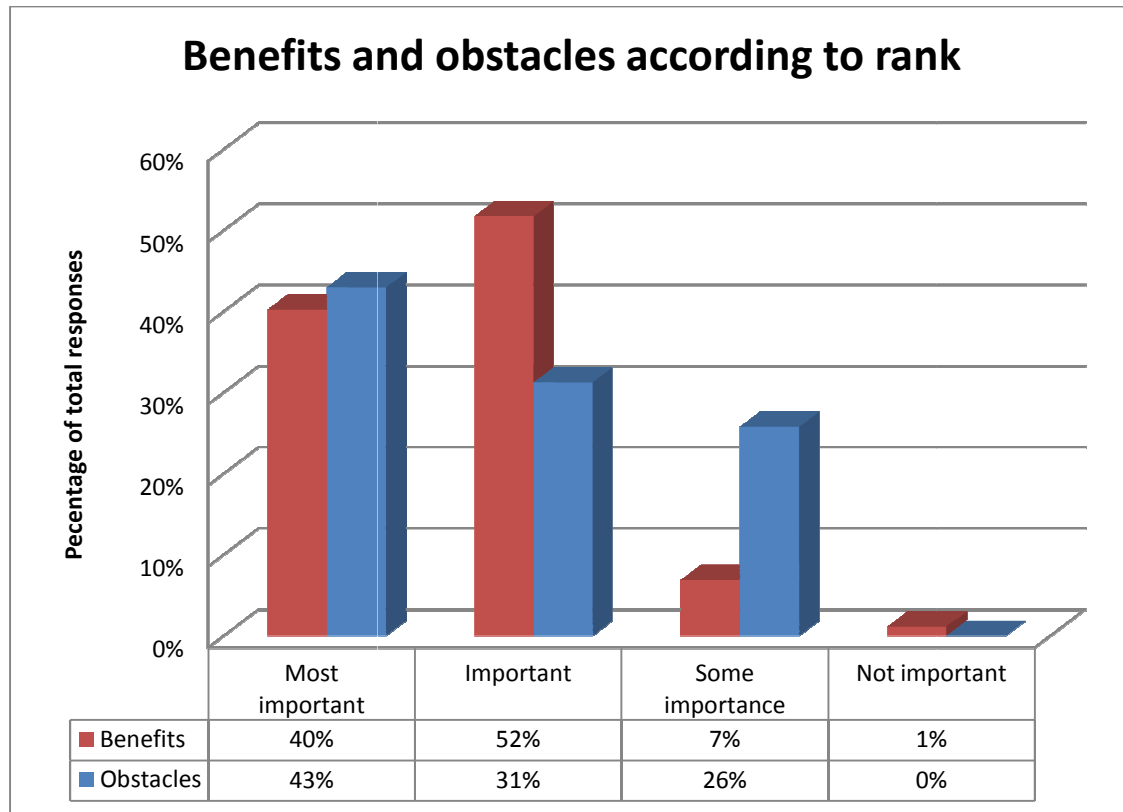**Summary of results for Question 1 according to categories**

Table 5.1

General	Service models	Deployment models
• Cloud is a pooled resource • Cloud is provisioning of capability with low capital investment • Allows one to focus on core business • A new concept for SA banks, currently a slow adaptor • Not a new concept in general, but a new way to deliver IT services and resources • Regulation should be taken into account especially in the financial services industry • Protection of Personal Information (POPI) should be taken into account in South Africa, also customer privacy • Cloud is an enabler of	**IaaS** • Infrastructure is a huge expense in the bank, thus need to see what can be moved to cloud, infrastructure layer should be in place though • Very relevant, as this service is bottom of the stack • Should be used for development and testing and be in public cloud **SaaS** • Non- core applications for e.g. HR, collaboration, email • Maybe suitable for smaller organisations as scale already exist in large banks • Email/exchange is still poses a risk or control issue for banks in South	**Private cloud** • Most relevant in the SA banking environment • Exist in storage and virtualisation space • Also known as an internal cloud • Core banking will be private cloud solutions • Not shared and control stays within the bank **Public cloud** • Access to all, external cloud • Not for SA banks currently • Explore for non critical/non core functions and applications • Legacy software is a huge hindrance for

speed and agility for e.g. speed to market, currently a bottleneck in banks • Mainframe already packaged as cloud • Cost reduction as you will only pay for utilisation of hardware and software services • Cloud provider - also a risk around indemnification	Africa • Limit to development and user acceptance testing (UAT) environment **PaaS** • Very relevant as the IP is in the application • Can enable innovation for e.g. new services and products by utilising of development tools • Life cycle management benefit	moving into the public cloud • Less capital layout • Security, privacy and governance/control still an issue • Also POPI to consider **Hybrid cloud** • Combination of a public and private cloud • Could be the best fit currently • Public cloud to be used at month end **Community cloud** • Where groups or communities have a shared interest • Cost is lower than a private cloud • Economies of scale

Question 2 and 3: Specific benefits and obstacles are mentioned in the cloud environment. Which are most important in a South African banking context?

Figure 5.1: Bar graph

Benefits and obstacles according to rank

	Most important	Important	Some importance	Not important
■ Benefits	40%	52%	7%	1%
■ Obstacles	43%	31%	26%	0%

Benefits in general are seen as either most important (40%) or important (52%), which accounts for 92% of total responses (figure. 5.1). Cost elasticity stands out as a benefit that is seen as most important in a SA bank (71%). Solutions follow with 45% as most important and 48% as important (figure. 5.2).

Resources and Service provider have some responses reflected as some importance with 13% each and 4% as not important reflected specifically for resources (figure. 5.2). Question two had one non-response for the solutions category.

Figure 5.2: Bar graph

Benefit categories according to rank

	Most Important	Important	Some Importance	Not Important
■ Resources	8%	75%	13%	4%
■ Solutions	45%	48%	6%	0%
■ Cost Elasticity	71%	29%	0%	0%
■ Service Provider	25%	63%	13%	0%
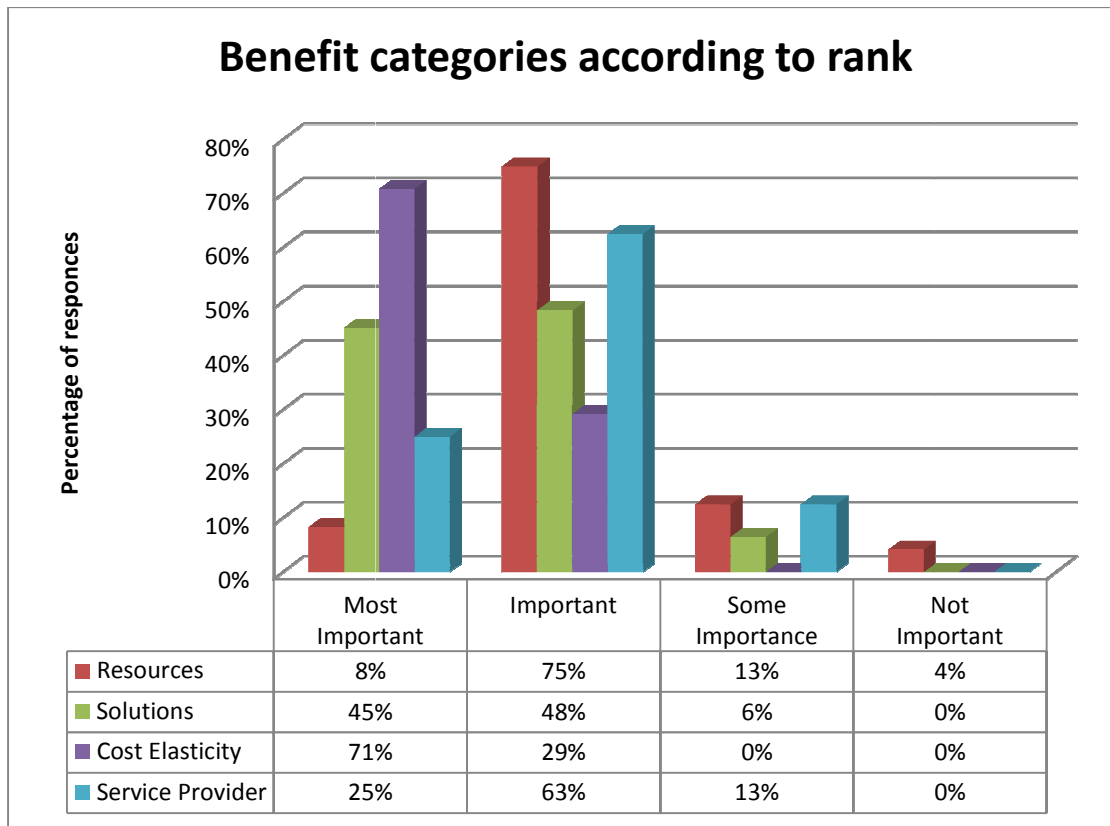
Other benefits seen as important by interviewees

Table 5.2

Interviewee	Other benefits
Interviewee 1 (GITS COO)	• Multi- National Companies (MNC's) will benefit as they can consider moving staff to medium and low cost locations as result of shared infrastructure, which takes away the presence of staff at different price points
Interviewee 2 (GTIS Co-Head)	• Agility for specifically projects where hardware is a requirement, it should reduce the turnaround/delivery time and lead to speed to market
Interviewee 3 (GTIS: Head of Engineering)	• None mentioned

Interviewee 4 (GTIS: Specialist Engineer)	• Early adoption in SA banking environment should lead to best service offerings from service providers but it can go the other way also
Interviewee 5 (GTIS: Manager Mobile)	• None mentioned

Interviewee 6 (Expert)	• Also have to look at drivers and motivators for cloud in SA bank environment.
	     o Drivers: Collaboration and alignment, growth in revenue and products/ services, operational efficiency
	     o Motivators: Cost reduction, focus on core, scalable infrastructure, agility – *time to market* for new products/ services and obtain competitive advantage

Interviewee 7 (GTIS: Co-Head)	• Access to skilled resources • Rapid deployment • Cost predictability
Interviewee 8 (Head of Technology: RBB and Digital)	• Time to market • Skills – the need for specialised skills • Economies of scale – driving price points down

Obstacles are seen as most important by 43 percent, important by 31 percent, which accounts for 74 percent of total responses. It is important to note that 26 percent of responses are reflected as 'some importance' for obstacles (fig. 5.1).

Privacy and security stands out as a category under obstacles with 94 percent of responses reflected as most important (fig. 5.4). Performance and reliability and service provider as categories follow with 53 percent and 50 percent respectively reflected as most important. It should however be noted that cost as obstacle is still seen as important (47 percent) and reflects an aggregated score of 69 percent for most important and important. More than 50 percent of responses (54 percent) for resources as category reflect only some importance.

Figure 5.4: Bar graph

Obstacle categories according to rank

	Most Important	Important	Some Importance	Not Important
Resources	17%	29%	54%	0%
Performance and reliability	53%	35%	13%	0%
Cost	22%	47%	31%	0%
Service Provider	50%	19%	31%	0%
Privacy and Security	94%	6%	0%	0%
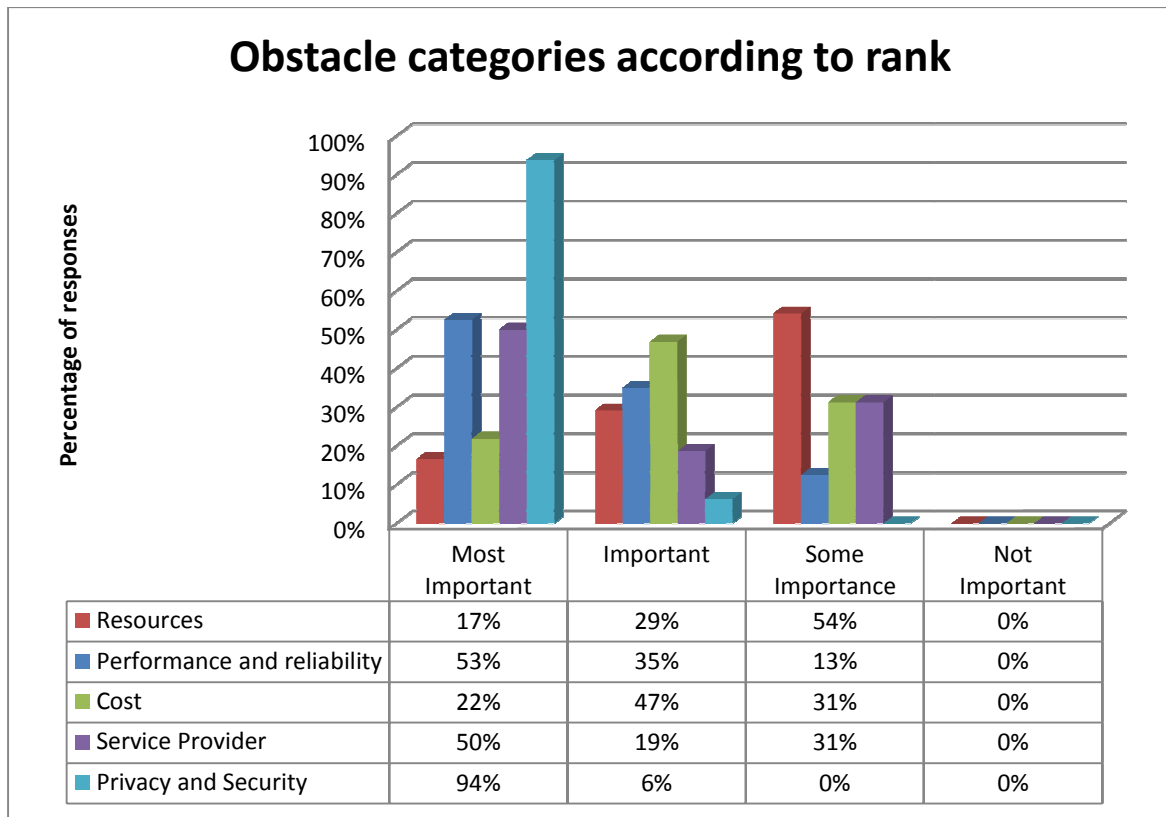
Other obstacles seen as important by interviewees

Table 5.3

Interviewee	Other obstacles
Interviewee 1 (GITS COO)	• Contractual negotiation with service provider • Disaster recovery – how to quickly get additional resources during a crisis event
Interviewee 2 (GTIS Co-Head)	• Lack of control in the cloud, have to change the mind-set of bankers • Retained organisation – jobs will be reduced and we have to create jobs in SA
Interviewee 3 (GTIS: Head of Engineering)	• None mentioned
Interviewee 4 (GTIS: Specialist	• None mentioned

Engineer)	
Interviewee 5 (GTIS: Manager Mobile)	• None mentioned
Interviewee 6 (Expert)	• Laws and regulations (ECA, PAIA, POPI and King 3) • Exit strategy from service provider-vendor lock-in • Audit and assurance – how cloud environment will be audited
Interviewee 7 (GTIS: Co-Head)	• Poor operational controls
Interviewee 8 (Head of Technology: RBB and Digital)	• Customer privacy - the onus is on the bank to safeguard the customers' data • Regulators- specifically the bank regulators' view of the risk of cloud for e.g. location of the cloud or physical presence of the cloud as the cloud can be anywhere

Question 4: Specific risks are being mentioned as part of cloud computing. Which are most important in an SA banking context?

Figure 5.5: Bar graph
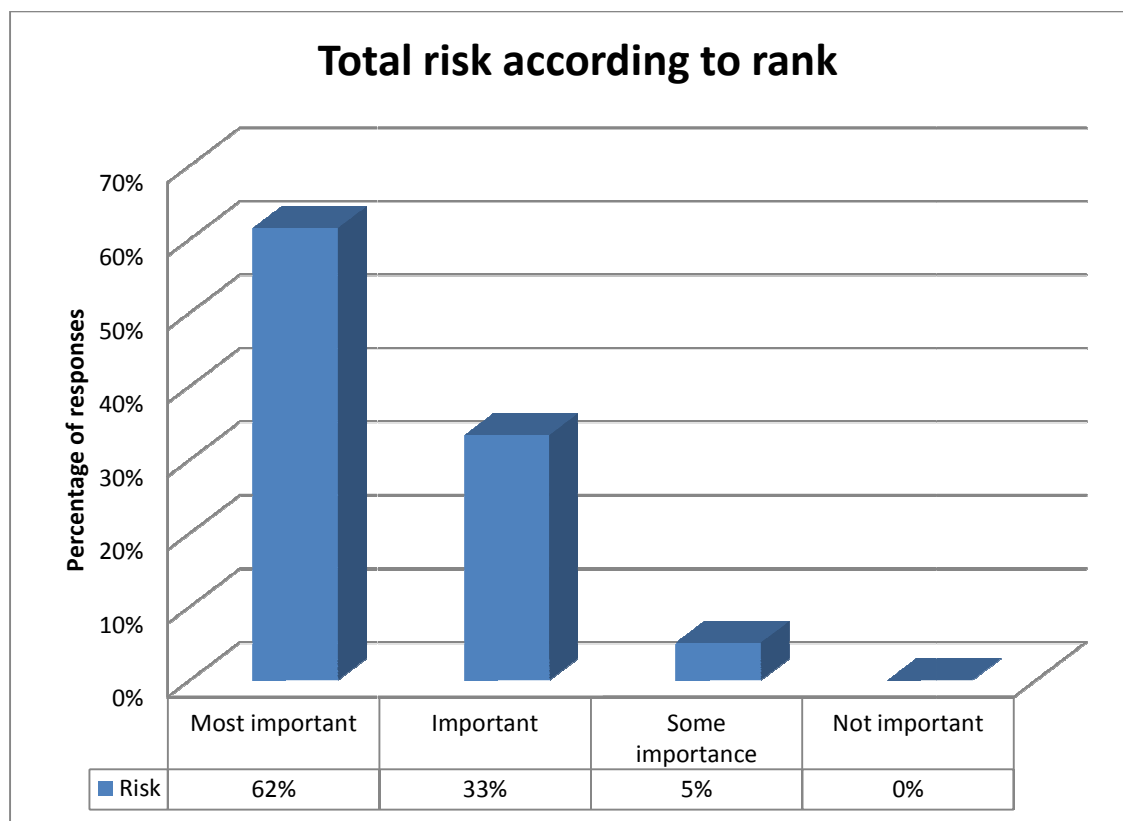
The 62 percent of responses for risk are reflected as most important, 33 percent as important and five percent as some importance (figure 5.5). Risk associated with infrastructure as category is seen as most important by 86 percent of interviewees (figure 5.6). All other categories under risk are seen as either most important or important by interviewees and 25 percent of interviewees reflected technical risk as category under risk as some importance (figure 5.6). Question 4 had one non- response for the risk associated with networks category.

Figure 5.6: Bar graph

Risk categories according to rank

	Most important	Important	Some importance	Not important
■ Policy and organisational risk	50%	50%	0%	0%
■ Technical risk	63%	13%	25%	0%
■ Legal risk	63%	38%	0%	0%
■ Risk associated with infrastructure for e.g. networks	86%	14%	0%	0%
■ Business and operational risk	50%	50%	0%	0%

Perecntage of responses (y-axis: 0%–90%)
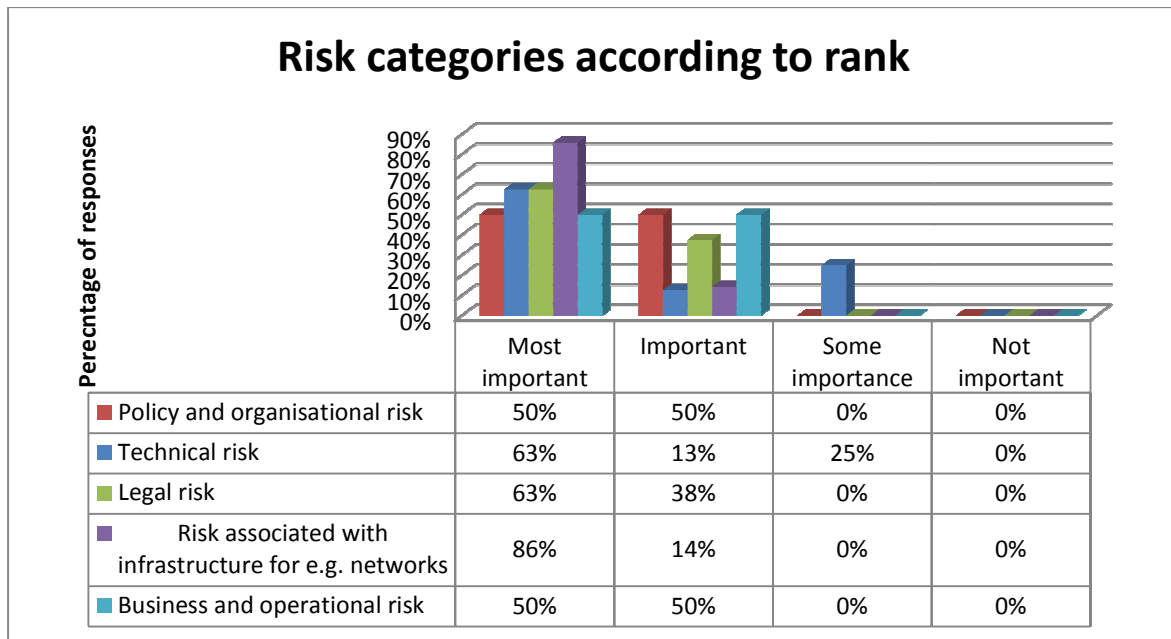
Other risks seen as important by interviewees

Table 5.4

Interviewee	Other risks
Interviewee 1 (GITS COO)	Regulatory risk from banking perspective
Interviewee 2 (GTIS Co-Head)	None mentioned
Interviewee 3 (GTIS: Head of Engineering)	None mentioned
Interviewee 4 (GTIS: Specialist Engineer)	None mentioned
Interviewee 5 (GTIS: Manager Mobile)	None mentioned
Interviewee 6 (Expert)	Vendor/ 3rd party risk around relationship, SLA, roles and responsibilities and exit strategies.
Interviewee 7 (GTIS: Co-Head)	Compliance risk
Interviewee 8 (Head of Technology: RBB and Digital)	Reputational risk for the bank if the cloud service provider do not perform

Question 5: Do the benefits of cloud computing in a SA bank outweigh the specific risks and or obstacles – why if yes or no? Also provide top three benefits and obstacles or risks.

Interviewee 1 (GTIS COO)

The risk of cloud computing do not outweigh the benefits, the cloud model makes sense as it is pooled resources that cost less to the organisation. It however also depends on the risk appetite of the organisations' shareholders.

Interviewee 2 (GTIS Co-Head)

The benefits of cloud outweigh the risks. There are a number of security tools available. Key is encryption of data in storage and when in transit. It is all about risk appetite, thus maybe start with email to save on software and infrastructure cost. The benefit of sharing is also important. More should be done to also move to public cloud in the bank.

Interviewee 3 (GTIS: Head of Engineering)

Benefits do not outweigh obstacles/risks. Security is still the problem, specifically in the public cloud around control issues. Core business is banking.

Interviewee 4 (GTIS: Specialist Engineer)

Benefits do outweigh obstacles/risks by far. The key is however to remove the obstacles as soon as possible. It should start with infrastructure being outsourced to a service provider.

Interviewee 5 (GTIS: Manager Mobile)

Obstacles/risks outweigh the reduction in costs as cloud is not a tried and trusted environment for banking. Considering costs it should however be tried in a scalable model in the future.

Interviewee 6 (Expert)

Can go public for certain services (non- core) such as CRM, Sales, email, HR and development and testing which are all collaboration services. Important is to identify the risks and mitigate these risks. It is also important to look at risk vs. reward and to clearly understand the risk universe.

POPI (Protection of Personal Information) will have a huge impact - when it becomes an act - on what banks can put in the public cloud and will have to default back to private cloud where service provider is in another country and they do not comply with local (SA) acts.

Interviewee 7 (GTIS: Co-Head)

Internal/Private cloud – we have to go cloud in the SA banking environment, it is inevitable.

External/Public cloud – selective opportunities exist which have to be carefully investigated. A sweet spot will be a cloud service provider providing a service on-site (the clients' site) for e.g. SaaS and PaaS.

Interviewee 8 (Head of Technology: RBB and Digital)

Public cloud – the benefits do not outweigh the obstacles/risks.

Private cloud – benefits in some instances do exceed the obstacles/risks. The opportunity is in the private cloud world for banks and specifically how to exploit this. There was a definite spike in VM installations since cloud came to the fore, as internal service provider had to adopt or go out of business as public cloud providers were offering the service. This then drove adoption of virtual environments in the bank. With private cloud you do not have to worry about consumption, billing and security layers.

Top three benefits and obstacles/risks

Table 5.5

Interviewee	Top three benefits	Top three obstacles/risks
Interviewee 1 (GTIS COO)	• Operational cost reduction • Capital layout reduction • Scalability	• Deterioration in service • Non DR • Privacy and security
Interviewee 2 (GTIS Co-Head)	• Cost reduction • Flexibility (time to deploy) • Maintenance of environment – outsourced to service provider	• None mentioned specifically
Interviewee 3 (GTIS: Head of Engineering)	• Infrastructure independent – do not have to host this internally • Cost of infrastructure lower – because service provider has shared infrastructure	• Security • Reliability – not guaranteed • Cost – locked/hooked in with service provider and cost not predictable
Interviewee 4 (GTIS: Specialist Engineer)	• Business agility – time to market (responsiveness) • More predictable operational cost	• Own internal governance – need to change (GIS, IRM) • Resources – soft issues.
Interviewee 5 (GTIS: Manager Mobile)	• Cost – infrastructure and resources • Auto disaster recovery	• Performance and reliability • Privacy and Security

Interviewee 6 (Expert)	• Enhanced collaboration (customers and employees) • Customer centric • Innovation (agility)	• Laws and regulations (POPI) • Security (information protection)
Interviewee 7 (GTIS: Co-Head)	• Cost • Time to deploy linked to operational efficiencies such as backup and failover • Less resource intensive but high skill level required • More leverage and handle on SLA, thus SLA better defined (commercial motive)	• External cloud-Information risk and operationally complex
Interviewee 8 (Head of Technology: RBB and Digital)	• Scale • Time to market • Less complexity around technology stack	• Fraud risk • Customer data and specifically privacy around the data. • Legacy in a private cloud

Question 6: What else should be considered as important around cloud computing in the South African banking environment?

GTIS COO

Reserve bank steer is needed in terms of regulatory issues and how will they feel? The financial stability of major banks in SA and that of the country itself might be at stake and to be considered. The principle should be what is best for the National Payment System and the risk exposure for the economy should the 'big five' move into cloud."

GTIS Co-Head

One hindrance to consider is that the Internet access penetration from a customer perspective still very low in SA for e.g. 12 million customers but only 1.3 million on Internet bank. Internet infrastructure is still very expensive in SA. Mobile is changing for the better though, but smart phones are not available and or affordable to average South African.

GTIS: Head of Engineering

No additional comments

GTIS: Specialist Engineering

A Mind-set change is required and people need to embrace cloud.

GTIS: Manager Mobile

No additional comments

Expert

No additional comments

GTIS Co-Head

> The SA market is still immature in terms of cloud computing. The risk of going off-shore is huge in terms of cost (FX differences) and stability for e.g. one bank took their credit card business off-shore and brought it back. The 'sweet spot' for any bank would be to go with SaaS on their own infrastructure. The ability to sustain 'bespoke' applications is very expensive on the long term and skills shortage is also a constraint with these applications.

Head of Technology: RBB and Digital

> Security and customer privacy issues should be resolved. Also what technologies can one apply to make it more feasible, thus what standards should be put in place to make it 'bullet proof'.
> It will take a 'brave man' from a banking perspective to put core banking in the public cloud.

The comments above from interviewees were categorised as below to summarise other key factors around cloud computing derived from interviewees.

- **Regulatory**

  > Reserve bank steer is needed in terms of regulatory issues and how will they feel? The financial stability of major banks in SA and that of the country itself might be at stake and to be considered. The principle should be what is best for the National Payment System and the risk exposure for the economy should the 'big five' move into cloud.

- **Internet Access**

  > One hindrance to consider is that the Internet access penetration from a customer perspective still very low in SA, for example, there are 12 million banking customers but only 1.3 million on Internet bank. Internet

infrastructure is still very expensive in SA. Mobile is changing for the better though, but smart phones are not available to the average South African.

- **Change Management**

    Mind-set change is required and people need to embrace cloud. The SA market is still immature in terms of cloud computing. The risk of going off-shore is huge in terms of cost (foreign exchange differences) and stability for example, one bank took their credit card business off-shore and brought it back.

- **Service and deployment model**

    The 'sweet spot' for any bank would be to go with SaaS on their own infrastructure. The ability to sustain 'bespoke' applications is very expensive on the long term and skills shortage is also a constraint with these applications.

- **Obstacles/Risks**

    Security and customer privacy issues should be resolved. Also what technologies can one apply to make it more feasible, thus what standards should be put in place to make it 'bullet proof'. It will take a 'brave man' from a banking perspective to put core banking in the public cloud.

6. Discussion of results

6.1 How should cloud be understood in a South African banking environment?

6.1.1 General

It is clear from the results that cloud computing is a new concept for South African banks. Cloud computing in general is understood in alignment with the various definitions identified in the literature reviewed for cloud computing. It is however apparent that in a bank environment in South Africa, issues such as regulation in the financial services environment and acts around protection of information should be taken into account when cloud is discussed. One recent act is POPI or the Protection of Personal Information act which will formally become an act when signed by the President of South Africa (IT Web, 2013). Cloud computing is also seen as an enabler for speed and agility in the banking environment in South Africa, but caution should be taken when a service provider is chosen, especially around indemnification.

6.1.2 Service Models

- **Infrastructure as a Service (IaaS)**

  IT Infrastructure is currently seen as a huge expense as part of total IT spend in SA banks, thus the question should be what can be moved into the cloud. De Nederlandsche Bank (DNB) has recently cleared Amazon Web Services (AWS) to be used in financial sector of the country (Brandon, 2013).

- **Software as a Service (SaaS)**

  SaaS is seen as suitable for non-core applications, smaller organisations as scale already exist in large banks in South Africa. Where SaaS is implemented though interviewees felt that preference should be given to non-core applications such as collaboration tools, email and HR systems.

46

- **Platform as a Service (PaaS)**

  PaaS was seen as very relevant, especially due to the fact that the intellectual property (IP) exist in the application itself. PaaS can also be an enabler for new services and products when development tools are utilised on such a platform service. A life cycle management benefit was also mentioned but the interviewee did not expand on this.

6.1.3 Deployment models

Private cloud also referred to as 'internal cloud' as deployment model is seen as the most relevant in a South African bank, which in some instances already exists in the storage and virtualisation space. Core banking solutions will currently be private cloud solutions as these are not shared and the control stays within the bank.

The public cloud as deployment model is not seen as a preferred deployment model for SA banks currently. It should however be explored for non-core functions and applications going forward. Legacy (bespoke) software together with security, privacy and governance issues are still seen as a huge hindrance for moving into the public cloud space in SA banks.

It was however pointed out that hybrid cloud solutions could be the best fit currently, where a public cloud deployment model is then used at month-end to cater for high volumes. It was also mentioned that potential economies of scale exists in a community cloud as a result of shared interests and that the cost is lower than that of a private cloud model.

6.2 What are the benefits of cloud computing in a South African bank?

Benefits as mentioned in the literature reviewed are seen as either most important or important in the SA banking environment, with 40 percent of total benefits reflected as most important and 52 percent reflected as important (figure 5.1).

Cost elasticity as benefit stands out with 71 percent and specific benefits under cost elasticity as category are reduction in capital layout, reduction in support and maintenance cost of infrastructure and lastly universal access to software and services with a related cost reduction as result. The fact that cost is so important in a SA bank is an indication of how important it is for banks in SA to drive cost down and achieve their target cost to income ratios. A report from Price Waterhouse Coopers (PWC) for the period ended 31 December 2012 mentioned that cost containment strategies in banks in SA will continue as a result of poor revenue growth (PWC, 2013).

Important however is to look at other benefits mentioned by interviewees that are not mentioned in the literature reviewed. The other benefits mentioned as per table 5.2 focuses on agility, time to market or turnaround time which can be grouped together. Also brought up was the benefit of the early adoption of cloud with possible best offering and/or service as reward.

Table 6.1 below indicates these other benefits identified for existing categories as identified from the literature reviewed and potential 'new' categories that emerged. Interviewee six specifically mentioned that one should also look at the drivers and motivators for cloud computing in the SA banking environment and these are presented in table 6.2.

Table 6.1

Category	Benefit
Resources	• Access to skilled resources • Low cost of resources – neutralisation of different price points where staff can be relocated low cost locations
Solutions	• Rapid deployment • Time to market is reduced for products and services
Cost	• Cost predictability
Service provider	• Best of service as result of early adoption

Table 6.2

Drivers	Motivators
Collaboration	• Cost reduction
Alignment	• Ability to focus on core business
Growth in revenue and products/services	• Scalable infrastructure
Operational efficiencies	• Agility – time to market for new products and services to obtain competitive advantage

6.3 What are the obstacles and risks of cloud computing in a South African bank?

6.3.1 Obstacles

Obstacles as mentioned in the literature reviewed are seen as most important by 41 percent of total responses and 31 percent as important which gives an aggregate score of 74 percent for total responses (figure 5.1). Privacy and security as a category stands out with 94 percent of responses being reflected as most important and six percent as important for an aggregate of 100 percent (figure 5.4). This response for privacy and security relates back to the fact that banks in general seems to be reluctant about cloud computing especially with regards to security and regulation (Banktech, 2010) and also question one where it was stated that regulation, privacy and security together with governance are seen as an hindrance for cloud computing, especially public cloud, in the SA banking context.

Performance and reliability is ranked second as category with an aggregate of 86 percent reflected for most important and important, followed by service provider (69 percent aggregate) and cost (67 percent aggregate) as categories.

Important to note is that only 46 percent as an aggregate for most important and important are reflected for resources and 54 percent for some importance. This indicates that resources are not seen as a huge obstacle for moving into the cloud, where it was seen as an important benefit with 75 percent of responses reflected as important.

Other obstacles not mentioned in the literature reviewed and therefore not ranked according to importance, are tabled in table 6.3 below under categories established from the literature reviewed for the analysis of the data. Where an obstacle does not fit one of the pre-defined categories it is reflected under a potential new category.

Table 6.3

Existing categories	
Resources	• Retained organisation – jobs will be reduced
Performance and reliability	• Disaster Recovery – how quickly can resources be provisioned in case of a crisis
Cost	• None
Service Provider	• Contractual negotiations
Privacy and security	• Customer privacy – the bank has to protect and safeguard the customers' data
New categories	
Change Management	• Mindset change is required
Governance and regulation	• Laws and regulation (ECA, PAIA, POPI and King 3) • Audit and Assurance – thus how cloud will be audited • How bank regulators will view the risk of cloud in South Africa for example the location of cloud

6.3.2 Risks

Risk is reflected as either most important or important by interviewees (figure 5.5). The risk associated with infrastructure as category is reflected as most important by 86 percent. This can probably be ascribed to the fact that interviewees were mostly from the IT sector and more specifically from the infrastructure department.

Other risks mentioned not covered in the categories as derived from the literature reviewed are vendor or third party risk mentioned by interviewee 6 (Expert) and compliance risk mentioned by interviewee 7 (GTIS Co-Head). Third party or vendor risk could be mitigated by ensuring that contracts with vendors are up to date and are regularly reviewed in terms of performance and exit clauses. Reputational risk was also

mentioned by interviewee 8 (Head of Technology: RBB and Digital) as a result of non performance by the service provider. Reputational risk could probably be seen as part of policy and organisational risk.

6.4 Do the benefits outweigh the issues and risks for cloud computing in a bank in South Africa?

Responses varied for this question and two interviewees, the head of engineering and manager mobile felt that the benefits do not outweigh the risk and obstacles of cloud computing in a SA bank. The head of engineering specifically mentioned that security is still a problem, specifically in the public cloud. The mobile manager said that cloud is not a tried and trusted environment for banking in SA, but considering costs it should be tried in a scalable model in the future.

All other interviewees were in some way in favour of the fact that the benefits do outweigh the obstacles and risks but with reservation in some instances. The GTIS COO mentioned the risk appetite of the organisation, which is also supported by one of the GTIS Co-heads. The specialist engineer mentioned that obstacles should be removed and that the start of moving into public cloud should be to move infrastructure to and outsourced service provider, which again is supported by the fact that the De Nederlandsche bank (DNB) has already moved infrastructure into the public cloud with Amazon as outsourced service provider (Brandon, 2013).

The Expert focussed on the fact that one can go public cloud for certain non-core services or collaboration services such as CRM, Sales, Email and Human Resources which should include development and testing. Risks should be identified and mitigation action should be put in place for these risks. Drivers and barriers should also be considered in the bank environment. POPI was again mentioned and the fact that when it becomes an act it will have an impact on the location of the service provider, especially if located in another country and they do not comply with SA acts and regulations.

Interviewee 7, the other GTIS CO-head distinguished between Private/Internal and Public/External cloud. He mentioned that SA banks have to go cloud in terms of private cloud but had some reservations in terms of the public cloud as selective opportunities will have to be investigated. He further mentioned that a 'sweet spot' will be if a cloud service provider can provide services on site (the clients' site) for example SaaS and PaaS.

Interviewee 8, the Head of Technology for RBB and Digital also distinguished between public and private cloud and indicated that for public cloud the benefits do not outweigh the obstacles and risks, but that it does for private cloud. He made mention of the fact that a result of cloud coming to the fore, there was a spike in VM installations, as internal service providers realised that public cloud providers were now also offering these services. Some benefits of a private cloud were also mentioned such as the fact that one does not have to worry about consumption, billing and security layers.

It is clear from the discussion above that there is a definite appetite for banks in SA to move into the cloud as most interviewees indicated that benefits do outweigh the obstacles and risks, but some reservations still exist about the public cloud.

Cost still comes out as one of the top three benefits, which support responses from Question two, for most interviewees when asked to identify their top three benefits and obstacles or risks with cloud computing in a South African bank. The focus around cost benefits seems to be reduction in capital layout, cost predictability and a reduction in operational cost to support infrastructure, software and services as these will be outsourced to a service provider. Also mentioned as a top benefit is business agility, which should lead to quicker time to market for products and services in general which is also prevalent as top benefit. Collaboration and customer centricity is also mentioned and customer centricity can probably be seen as part of collaboration.

Issues around security and privacy (also customer data), laws and regulation, governance, information risk (external cloud) feature as some of the top obstacles or risks mentioned, which is supported in general by responses from question three.

The opinion of the researcher is, that research objectives as set out in chapter three, have been met.

6.5 Concerns

It is important to note that the sample was only limited to eight interviews in one of the major banks of SA. It would be misleading to use the results from this research to draw conclusions about the total population.

7. Conclusion

The research conducted on cloud computing in a SA bank was based on existing theory which were collected by an in depth literature review specifically around the definition of cloud computing, the service and deployment models and the benefits and obstacles of cloud computing. The attempt with the research study was to find out if banks in South Africa can identify with specific deployment and service models for cloud computing and if benefits, obstacles and risk as identified from the literature reviewed are relevant to them. One of the four major banks in SA was selected as a homogenous sample. Eight interviews were conducted in the bank, specifically the IT sector of the bank.

The research conducted indicates that in some aspects cloud, as a concept, is still new to SA banks, although this seems to be more accurate in the case of the public cloud. The indication from the research is that private clouds have been in existence for quite some time in SA banks in the form of either data centres or virtualisation.

Reluctance to move into or deploy into the public cloud is mainly as a result of issues such as privacy and security, laws and regulations and also the factor of the great unknown. POPI is one example that was presented around laws and regulation which is expected to have a huge impact of what will be in the cloud in the financial services industry, especially the public cloud. Important to note is that cloud computing is seen as an enabler for speed and agility, especially with time to market for new products and services.

In terms of service models the research indicated that IaaS should be first priority to move into the public cloud domain, but that it will be governed by laws and regulations. PaaS was also seen as very relevant as the intellectual property (IP) is not with the service provider who provides the platform but in the application itself.

The research indicated that SaaS is probably more suitable for smaller organisations, as some scale already exists in larger banks in SA. If implemented however it should be focused on non-core applications such as collaboration tools.

Benefits in the cloud for SA banks were evaluated in line with benefits as identified form the literature reviewed, with cost and all its aspects being identified as the most important benefit in a bank. Other benefits emerged such as cost predictability, time to market, rapid deployment, access to skilled resources and low cost of resources due to elimination of different price points especially in Multi National Companies (MNC's).

Obstacles in the cloud were also evaluated in line with obstacles as identified from literature reviewed and privacy and security were identified as the most important obstacle to consider in a bank in SA. The research also indicated that resources is not seen as a huge obstacle for moving into the cloud although mentioned as other obstacles was the fact that a reduction in resources will have to be managed inside the organisation. Other obstacles that emerged are contractual issues with the service provider, customer privacy which is a huge obstacle for a bank in terms of laws and regulation and to exist as a going concern. One potential new category that emerged is change management, thus how to motivate staff and also manage potential reduction and movement of staff to the outsourced service provider. Another potential category that emerged is governance and regulation especially in terms of ECA, PAIA, POPI and King 3. It is also important going forward to understand how cloud computing will be viewed by the bank regulator.

The research indicated that risk is seen as most important and especially risk in terms of infrastructure. Important however is how specific risk is mitigated to ensure proper management of specific risks identified.

The research indicated that interviewees are in favour of cloud computing in terms of benefits outweighing obstacles and risks but that the focus should be on private cloud and that only some services can be put in the public cloud.

Collating the general feeling derived from interviewee's, other issues to be looked at, or that should be considered, before banks in SA can move into the cloud are: regulatory issues, internet access, change management and the service and deployment models.

This also provides an indication of possible future research that can be conducted for cloud. Potential future topics could focus on:

- Cloud computing and laws and regulation in South Africa, specifically the impact of laws and regulation on cloud computing in the financial services industry
- What are the drivers and motivators for moving into the cloud and how does one identify these for an organisation
- Cloud computing and change management, how should the mindset (culture) be changed in the organisation
- Contract negotiation with cloud service providers, how should these contracts look when compared with standard service provider contracts?

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & ... Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM*, *53*(4), 50-58.

Berman, S. J., Kesterson-Townes, L., Marshall, A., & Srivathsa, R. (2012). How cloud computing enables process and business model innovation. *Strategy & Leadership*, 40(4), 27-35. doi: 10.1108/10878571211242920

Brandon, J. (2013, August 1). Dutch regulator okays Amazon Web Services for financial sector. *banking technology*. Retrieved from http://www.bankingtech.com/

Brynjolfsson, E., Hofmann, P., & Jordan, J. (2010). Cloud Computing and Electricity: Beyond the Utility Model. *Communications of the ACM*, *53*(5), 32-34.

Chin-Nung, L., I-Liang, C., & Yan-Kai, F. (2011). Cloud computing: A conceptual framework for knowledge management system. *Human Systems Management*, 30(3), 137-143. doi: 10.3233/HSM-2011-0746

Creeger, M. (2009). CTO Roundtable: Cloud Computing. *Communications of the ACM*, *52*(8), 50-56.

Crosman P. (2010, Aug 16). BS&T Survey: Banks Take to Cloud Computing. Retrieved from http://www.banktech.com/architecture-infrastructure/bst-survey-banks-take-to-cloud-computing/226100004

Cusumano, M. (2010). Technology Strategy and Management: Cloud Computing and SaaS as New Computing Platforms. *Communications of the ACM*, *53*(4), 27-29.

Durkee, D. (2010). Why Cloud Computing Will Never Be Free. *Communications of the ACM, 53*(5), 62-69.

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success Factors for Deploying Cloud Computing. *Communications of the ACM*, *55*(9), 62-68. doi:10.1145/2330667.2330685

Gartner (n.d.), Cloud Computing. Retrieved from http://www.gartner.com/technology/topics/cloud-computing.jsp

Gartner (n.d.). Worldwide IT Spending Forecast, 1Q13 Update. Retrieved from http://www.gartner.com/technology/research/it-spending-forecast/

Gold, J. (2012). Protection in the cloud: Risk management and Insurance for cloud computing. *Journal of Internet Law*, 15(12), 1-28.

Greengard, S. (2010). Cloud Computing and Developing Nations. *Communications of the ACM*, *53*(5), 18-20.

Growing in an uncertain world, South Africa – Major banks analysis. (2013). Retrieved from http://www.pwc.co.za/en/assets/pdf/south-african-banking-analysis-march-2013.pdf

Guptill, B., & McNee, W. S. (2008). SaaS sets the stage for 'Cloud Computing' (cover story). *Financial Executive*, *24*(5), 37-44.

Hayes, B. (2008). Cloud Computing. *Communications of the ACM*, *51*(7), 9-11.

Kalyvas, J. R., Overly, M. R., & Karlyn, M. A. (2013). Cloud Computing: A Practical Framework for Managing Cloud Computing Risk--Part I. *Intellectual Property & Technology Law Journal*, 25(3), 7-18.

Lin, A., & Chen, N. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, *32*(6), 533-540. doi:10.1016/j.ijinfomgt.2012.04.001

Mackay, M. M., Baker, T. T., & Al-Yasiri, A. A. (2012). Security-oriented cloud computing platform for critical infrastructures. *Computer Law & Security Review*, 28(6), 679-686. doi:10.1016/j.clsr.2012.07.007

Mishra, A., Jain, R., & Durresi, A. (2012). Cloud computing: networking and communication challenges. *IEEE Communications Magazine*, 50(9), 24-25. doi:10.1109/MCOM.2012.6295707

Patton, M. Q. (2002). Qualitative research & evaluation methods (3rd ed.). Thousand Oaks, CA: Sage Publications.

Rader, D. (2012). How cloud computing maximizes growth opportunities for a firm challenging established rivals. *Strategy & Leadership*, 40(3), 36-43. doi: 10.1108/10878571211221202

Ryan, M. D. (2011). Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM*, *54*(1), 36-38. doi:10.1145/1866739.1866751

Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network & Computer Applications*, 35(6), 1831-1838. doi:10.1016/j.jnca.2012.07.007

Srivastava, K., & Kumar, A. (2011). A New Approach of Cloud: Computing Infrastructure on Demand. *Trends in Information Management*, *7*(2), 145-153.

Sultan, N. (2013). Cloud computing: A democratizing force? *International Journal of Information Management*, 33(5), 810-815. doi:10.1016/j.ijinfomgt.2013.05.010

von Solms, R. R., & Viljoen, M. M. (2012). Cloud computing service value: A message to the board. *South African Journal of Business Management*, *43*(4), 73-81.

Zhang, Y., Li, Y., & Zheng, W. (2013). Automatic software deployment using user-level virtualization for cloud-computing. *Future Generation Computer Systems*, 29(1), 323-329. doi:10.1016/j.future.2011.08.012

Appendices

Appendix 1: Informed consent letter and interview schedule

Informed consent letter:

I am conducting research on cloud computing in South African (SA) banks, and am trying to find out more about the how cloud is understood in SA banks, what are possible benefits and obstacles of cloud in SA banks and if benefits outweigh the obstacles. Our interview is expected to last about an hour, and will help us understand how cloud computing is understood/defined in SA banks. Your participation is voluntary and you can withdraw at any time without penalty. Of course, all data will be kept confidential and no names of persons or specific institutions will be mentioned. If you have any concerns, please contact me or my supervisor. Our details are provided below.

Researcher name	*Research Supervisor Name*
Email	*Email*
Phone	*Phone*

Signature of participant: _____

Date: _____

Signature of researcher: _____

Date: _____

Interview schedule

1. How should cloud computing be understood or defined, especially in the SA banking environment?

General

Service Models (SaaS, PaaS and IaaS)

Deployment models (Public, Private and Hybrid)

2. Specific benefits are mentioned in the cloud environment such as..., which are most important/ beneficial in the SA banking context.
- Are there any other benefits that should be considered in a SA banking context?
- Resources, solutions, cost and SP – rank key themes and specific benefits under each key theme.

Benefits	Most important	Important	Some importance	Not important
Resources • Elasticity • Minimise staffing Less power usage(electricity)				
Solutions • Methodical and not random • Infrastructure scale automatically • Automatic disaster recovery • Quick application development and adoption				
Cost • Elasticity • Reduction in Capital expenditure/layout • Reduction in support and maintenance cost of infrastructure				

• Universal access to software and services – to reduce need for licenses and related cost.				
Service Provider • High service levels – especially with cloud 2.0 for e.g. offerings such as housekeeping and support				
Any other benefits				

3. Specific obstacles are mentioned as being part of implementing cloud computing, do you agree with these obstacles? Which of these obstacles are most important to take cognisance of and are then any other obstacles to consider in the SA banking context?

Obstacles	Most important	Important	Some importance	Not important
Resources • **Adaptability** to scale quickly • Scalable storage not a given • Illusion of infinite computing resources available				
Performance and reliability • Availability/Business continuity • Unpredictable performance • Bottlenecks with data transfer • Bugs in the cloud • Lack of constant high speed internet				
Cost • Adaptability to scale quickly • Scalable storage not a given • Small capital expenditure – is this really the case? • Pay for service as needed and on usage basis, easy to dispose or release when no longer required – is this really the case?				

Service provider • Perfect competition from a cloud service provider perspective • Expectation of low cost with cloud services and related conduct by the service provider.				
Privacy and Security • Privacy – accidental or deliberate disclosure of data and how does one protect data in the cloud? • Lack of control and loss of control which links to security and privacy issues.				
Any other obstacles				

4. Specific risks are mentioned as being part of cloud computing, do you agree with these and what other risks are important in the SA banking context? – ask to rank in order of importance.

Risks	Most important	Important	Some importance	Not important
Policy and organisation risk				
Technical risk				
Legal risk				
Risk associated with infrastructure for e.g. networks				
Business and operational risk				
Any other risks				

5. Do the benefits of cloud computing in a SA bank outweigh the specific risks and obstacles - why if yes or no? Ask interviewee's to rank order (top five benefits and obstacles/risks) and give a weighting (importance) to score benefits, obstacles and risks.

Benefits	Rank	Weight/Impact	Score	Obstacles/risks	Rank	Weight/Impact	Score

6. What else should be considered as important around cloud computing in the SA banking environment?

Appendix 2: Consistency matrix

Research Questions	Literature Review	Data Collection	Analysis
1. How should cloud be understood in a South African banking environment?	Srivastava and Kumar (2011)	Unstructured Interviews	Categorise data in to themes and link selected units such as sentences to the categories
2. What are the benefits of cloud computing in a South African bank?	Ambrust et al. (2010); Durkee (2010); Ryan (2011); Srivastava and Kumar (2011) and Lin and Chen (2012)	Semi-structured Interviews	Categorise data in to themes and link selected units such as sentences to the categories
3. What are the obstacles and risks of cloud computing in a South African bank?	Ambrust et al. (2010); Durkee (2010); Ryan (2011); Srivastava and Kumar (2011) and Lin and Chen (2012)	Semi-structured Interviews	Categorise data in to themes and link selected units such as sentences to the categories
4. Do the benefits outweigh the issues and risks for cloud computing in a bank in South Africa?		Semi-structured Interviews	Categorise data in to themes and link selected units such as sentences to the categories