A Proposed Framework to Assess and Increase the Cloud Computing Readiness of Financial Institutions in South Africa

Akinlolu Olumide Akande
Department of Information Systems
University of Cape Town
Cape Town, South Africa
Akinlolu.Akande@uct.ac.za

Jean-Paul Van Belle
Department of Information Systems
University of Cape Town
Cape Town, South Africa
Jean-Paul.Vanbelle@uct.ac.za

***Abstract*— Among the various industry sectors, the financial industry in South Africa (SA) has been one of the early adopters of cloud computing (CC) but they have not fully implemented it because of barriers such as security and privacy, governance issues, inadequate cloud service level agreements (SLAs), vendor lock in, poor vendor transparency, inability to assess risks, confidentiality, integrity and availability. Few guidelines exist to help organizations improve their CC readiness level. This is particularly risky for financial institutions that deal with sensitive customer information as the safety of that information is not guaranteed if a desired readiness level is not attained before implementation. In order to assist financial institutions with this hurdle, this paper proposes a framework that will serve as a tool by which financial institutions can determine and improve their CC readiness. The framework is called "Becoming Cloud Computing Ready" (BCCR) and it would help financial institutions to determine which stage they are with their CC readiness. It will also provide guidelines that will assist financial institutions to improve their level of readiness in order to ensure successful CC adoption. The proposed framework is grounded in both the literature as well as empirical data obtained from interviews with the largest financial institutions in SA.**

***Keywords—cloud computing; framework; readiness; organisational adoption; implementation; technology-organization-environment; financial institutions; South Africa*.**

I. Introduction

Cloud Computing (CC) provides convenient and immediate network access to a shared pool of configurable computing resources including servers, networks, applications, storage, and services that can be set up quickly and released with minimal service provider interaction or management effort [1, 3]. CC is becoming popular among organizations looking for cheaper ways to access needed infrastructure, applications and/or service. As a result, CC has changed organizations' perception of software, infrastructures and development platforms [2].

Although CC offers many benefits, there are some issues with CC which affects the adoption rates of financial institutions in SA. Some of these issues include uncertainty about data availability, possibility of vendor/data lock in, uncertainty about integrity, data privacy and confidentiality, security issues, lack of clarity on the perceived risks of cloud services as well as poor band width. Because of these issues, South African financial institutions have been slow to adopt CC. In addition, many do not know what needs to be in place in order to be ready for CC implementation, and no concrete framework exists to let financial institutions assess their CC readiness.

It is important for organizations to attain a high level of readiness before adopting a technology as a lack of readiness before adoption may lead to implementation failure. As a result, it is important for organizations to attain a high level of readiness before adopting CC. This paper proposes an integrated framework that will serve as a tool by which financial institutions can measure their CC readiness. The framework is based on both theoretical insights from the literature as well as empirical data which arose from a number of interviews with key CC decision makers in the top South African financial institutions.

The remainder of this paper sets out the key concepts and insights from the literature, followed by the research methodology. The bulk of this paper is devoted to discussion of the proposed framework.

II. Cloud Computing Definition and Issues

CC is a model that provides access to resources such as hardware, software and application to users on a pay as you go basis over the internet. CC is characterized by virtualization, automatic adaptation, user friendliness, internet centric, resource optimization, variety of resources, service-level agreements (SLAs) and infrastructure SLAs. Although CC provides many benefits, it is not without limitations. It is important for organizations to be aware of these limitations and take necessary precautions to prevent problems which may arise as a result of these limitations [4].

The issues with CC include the possibility of users being tied with one cloud provider due to lack of standardized application programming interfaces (APIs). Other issues include security issues, privacy issues, computing components are tightly coupled, user interface is not flexible and inability to support multiple tenants [5]

Because CC offers more benefits than disadvantages and limitations, many organizations are adopting CC while others

978-1-4799-4236-7/14/$31.00 ©2014 IEEE

are earnestly considering CC adoption. In the 2011 corporate cloud survey, one hundred large corporations listed on the Johannesburg Stock Exchange (JSE) in SA were interviewed. Forty six percent (46%) had already adopted CC while six percent (6%) planned to adopt it in 2012. Another four percent (4%) planned to adopt in 2013 [6]. Thirteen percent (13%) of the total sample said they didn't see any benefit of CC for their company and as a result, CC was not important for their business. Others are not planning to adopt CC because of poor infrastructure or security concerns but this is mostly because they are inhibited by their lack of understanding of CC [6].

III. Cloud Computing and Financial Institutions

CC adoption rate of financial institutions is low because of issues such as security, loss of control over data, data privacy, lack of standard SLA's etc. that are documented in literature. The fear that financial institution may be dependent on the service provider is another reason why financial institutions have been slow in the adoption of CC [7].

Although the adoption of CC by financial institutions has been slow, CC is not new to financial institutions. Many financial institutions have adopted some form of CC but they have been selective in their choice of CC because of concerns about CC. The earlier form of CC adopted by SA financial institutions was Software as a Service (SaaS) which was used for social media banking [8]. Other CC services used by financial institutions include collaboration, CRM systems, desktop and e-mail systems [7].

A. Benefits of cloud computing to financial institutions

CC offers facilities such as email, web hosting and fully managed applications which enhances communication between financial institutions and clients [8].

With CC, financial institutions can outsource their information technology (IT) operations and infrastructure to a service provider. This would allow them to concentrate on their business and not IT. Availability of service level agreements (SLAs) will ensure service delivery and availability by cloud providers. Operational risk and risk management costs can also be reduced by CC [9].

CC provides financial institutions with the opportunity to scale up or down based on customer's demand. This will eliminate the need to acquire and maintain the resources that are not needed thereby helping them to save on cost [8].

Furthermore, financial institutions can increase their performance through CC in a number of ways. Firstly, financial institutions can avoid large upfront cost of buying their own in-house technology through the use of CC. They can also select needed services and applications and pay per usage [8].

CC will also help financial institutions to achieve a higher level of data protection and fault tolerance. Disaster recovery can also be achieved by financial institutions at no extra cost because the responsibility of managing CC lies with the service provider.

Product development cycle of financial institutions can also be reduced by CC. This is because CC helps to save time by eliminating the need for purchase and installation. CC also helps to save the time necessary to maintain infrastructure. This allows financial institutions to pay more attention to their business and reduce their focus on IT. As a result, they are able to attend to their customers' needs in a timely manner [8].

B. Cloud computing risks for financial institutions

The dependence of CC on the internet is an important factor that financial institutions need to consider. If there is a problem with the internet, it would interrupt CC services. This could be expensive for financial institutions especially in departments that need real time information. For example, exchange rate departments [8]. There might be difficulty in moving applications across from one service provider to another as the service provider is responsible for backup and recovery of data [10].

Financial institutions also need to consider legal issues relating to data ownership and access. For example, if there is a court order or government officials request the service provider to give them access data to conduct investigations, several legal issues may arise. As a result, financial institutions need to know how to handle such situations so as to protect their customer's right to privacy and be able to retain the trust their customers have in them [11].

Finally, financial and customer information regarding transactions are important to financial institutions. Data should be protected from getting to unwanted parties. It should also be protected from intentional or accidental loss as well as leakage so that the reputation of the financial institution can be protected and to increase the customer's confidence [2].

IV. Considerations for organisations before moving into the cloud

The key factors that organizations need to consider before moving into the cloud include size of the IT resources and the utilization pattern of the resources. They also need to determine how sensitive their data is. For example, for data that is confidential, they may prefer to adopt private cloud. This will give them control over their data as they will have their own data center and have total control over it. For less sensitive data, they may prefer to use public cloud where the cloud provider will own the data center and have more control of data. The last factor is the criticality of work done by the company [12].

Organizations should consider these factors thoroughly before implementing CC as this will help them to determine what type of cloud services to adopt. These characteristics have been grouped based on the Technology, Organization, and Environment (TOE) framework [13] which was the selected framework for this research in order to add a profound theoretical stance to this research.

A. Technology

Organizations should ensure the availability of the entire necessary *ICT infrastructure* to support CC before deciding to adopt CC. This includes making sure that necessary technologies and expertise to operate those technologies are in place.

The *knowledge and awareness* of an organization about a technology is important for the success of implementation. If an organization is aware of a technology, they will be able to make necessary preparations before adoption and this will increase the success of their implementation.

B. Organisation

The *size of organizations' IT resources* is an important factor in determining whether an organization is ready for CC or not. This will help the organization to determine which type of CC to adopt. Private cloud may be better for organizations that already have their own data center and necessary IT infrastructure. This will improve security and privacy and confidentiality of their data will also be ensured as the organization will have total control of their data. The number of servers the company owns, number of their customers, annual IT revenue, and the number of branches and countries where they are located should be considered in order to determine the size of the IT resources of an organization [12].

The *utilization pattern of resources* should be considered by looking at the peak and average usage as well as the amount of data transactions done [12]. For example, organizations with resources that are not fully utilized may need to move into cloud so as to cut the cost of maintaining the unused resources. This will allow them to only pay for the utilized resources. This will help the organization to reduce waste by maximizing the use of their resources and as a result, the organization can save a lot on cost. Bandwidth consumption should also be considered because organizations that handle a large amount of data will require a large bandwidth to process and store data in the cloud. This means that they will spend a lot of money on bandwidth. It is therefore advisable for them to determine their bandwidth usage before implementing CC as the cost of CC may end up being more than the cost of their traditional systems in the long run [12].

Organizations that deal with *sensitive and confidential data* should carefully identify what to move into the cloud and what should remain on their traditional systems. Sensitive data could be moved into private cloud while less sensitive data could be moved into public cloud. This will help them ensure the security of their data [13].

Highly critical work needs stringent resources, platforms, applications and security [12]. Highly critical work also demands very rigorous SLA's and since SLA's are not yet standardized for CC, organizations need to be careful when performing their critical work on the cloud.

Support from top management is another important factor to consider before implementing CC as the success of CC implementation depends of top management's willingness to make necessary resources available for CC implementation [14].

CC requires some *special skills* to be implemented successfully. These include negotiation skills and management skills. Organizations should ensure training for their employees to ensure that the employees possess necessary skills to implement CC successfully. These skills include SLA negotiation skills, technical skills, training skills, server provider management skills, security skills, knowledge of laws and regulations, project and change management skills, business and finance skills, enterprise architecture and business analysis skills as well as data integration and analysis skills.

C. Environment

Legislation is an essential part of readiness. Organizations need to have knowledge of existing laws and legislation about CC. By doing this, they will know what to do whenever the service provider is in breach of the SLA. It will provide them with knowledge of their privacy and information protection. In cases where the data center and the organization are located in different countries, organizations need to know their rights and obligations in case of a breach and their information is visible to an unwanted party.

Every organization needs to conduct research and find out how to differentiate themselves from their competitors using CC. They also need to find out how to use CC to improve their business processes in order to increase their return on investment. They should not implement CC just because other organizations are implementing it. Most organizations fail in their CC implementation because they have little or no technical knowledge about CC and are not ready for CC [11]. Organizations need to implement CC for the right reasons and be motivated by the benefits it will offer them as this will contribute to the success of their CC implementation.

National infrastructure like bandwidth, internet facilities and other infrastructures that supports CC should be investigated by organizations. This will ensure that they make proper arrangements to guarantee continuous access to services, infrastructure, and applications subscribed for without any interruptions due to poor infrastructure [14]. Once organizations are sure that necessary infrastructure is available, they can then decide to move some or all of their data into the cloud.

V. Research Methodology

The framework was developed using inputs from the literature (partly summarized above) as well as an extensive empirical database [15]. A qualitative research approach was found to be the most appropriate for this research because of its ability to provide a strong foundation for the analysis and interpretation of data in the business environment. Semi-structured interviews were used because they allow participants to express themselves freely. This research adopted thematic analysis method because it has been found to be efficient in analyzing textual and qualitative data [19].

Participants were selected from banks and insurance companies in SA based on their size, number of customers and number of employees in order to obtain a sample that could be representative of financial institutions in SA. Participants were also selected from consulting firms that work for financial institutions and insurance companies and are involved with making most of their IT decisions for them. This was a very useful form of triangulation as it allowed the researchers to verify the data obtained from the banks and insurance companies from an external observer with good knowledge of the industry and CC. Although, the sample size was relatively small, it is important to note that the result of this research should be representative because the sample consists of majority of the industry players and accounts for most of the market.

The duration of each interview was between 1 to 2 hours. All the participants had knowledge of CC and are involved in making IT decision in their respective organizations. The number of employees in the participating organizations ranged from 500 + to 40000+. The researchers were able to analyze all the issues discussed using the TOE framework.

The data analysis identified the barriers and enablers of CC. This is consistent with the findings of [16]. The factors used to develop the proposed framework were also identified during the data analysis. These are used below. The level of CC readiness of SA financial institutions was also found to be low and is still in the early stages as most of the financial institutions have not made provisions for all the readiness factors. Some of these are reported in [17].

VI. The proposed "Becoming Cloud Computing Ready" BCCR framework

This section presents the proposed framework called "Becoming Cloud Computing Ready" (BCCR). The framework was developed based on a combination of the TOE framework, the change management framework [18] and the data obtained during the interviews. The framework is aimed at assisting financial institutions in SA to determine their level of CC readiness and help them improve their CC readiness level which will adversely improve their CC adoption success.

The first step towards readiness assessment is that organizations should understand why they want to adopt CC. They should ask themselves what values they want to derive from cloud computing and what the risks and challenges are.

Then they should consider how the impact of CC adoption on their organization compares with the suitability. For example, if it's low impact and it's highly suitable for their organization, then they are more ready than if its high impact and low suitability. If the decision is that CC will have a low impact and high suitability for the organization, they can proceed with their CC readiness assessment. The BCCR framework can then be applied to determine the organizations readiness and improve it if necessary. Figure 1 shows the BCCR framework and the relationship among all the factors that affects CC readiness.

To summarize the framework, note that technology and environment have a direct impact on the organization and would affect the organizational CC readiness. It also shows that the organizational factors have a direct impact on CC readiness and the CC readiness of organizations also have a direct impact on their CC adoption and implementation success. Change management should be applied at every stage of CC implementation right from the readiness assessment stage through to the adoption and implementation stage.

A. *Change Management*

The three steps for managing change successfully by [18] should be applied in all the stages as it will help to persuade and motivate people to help implement change. It will also make people feel more committed to making the change happen thereby increasing the CC readiness level of the organization and consequently increase their success of CC adoption.

Steps 1 and 2 of [18]'s three steps for managing change successfully should be applied during stage 1 (impact and suitability analysis stage) of BCCR framework. The manager or change agent should identify the expected type of resistance and determine his relationship with people who are expected to resist change. The manager or change agent should also determine whether the change is urgent or not. The manager or change agent also needs to determine whether the change will be intensive or not. This will determine whether the change should be carried out slowly or quickly. The organization can now proceed to do an assessment based on technology, organization and environment.

In stage 2 of BCCR framework, the manager or change agent should apply steps 2 and 3 of [18]'s three steps for managing change successfully. The optimal speed of change should be determined and methods for managing change should be considered. If the needed resources are available and there is top management support, this could mean that the change can be carried out quickly. If the staffs are satisfied with the existing system, they should be allowed to participate in designing and implementing the change as this will let them see the reasons for change and increase their commitment to change. Finally, participation, facilitation, negotiation and coercion should be applied if there is a decrease in job satisfaction. Participation will assist in reducing resistance to change by staffs that might be affected by the change. Facilitation will provide emotional support and training for staffs and provide them with skills that will help them cope with change. This will help increase job satisfaction. Negotiation will also help increase job satisfaction because staffs will be motivated if incentives are offered during negotiation. Coercion can be applied if other methods prove ineffective. Staffs that are still not satisfied could be threatened with possible loss of jobs or promotion opportunities.

The arrow that links stage 1 and stage 2 of BCCR framework indicates that CC would have low impact and high suitability for the organization and the organization can proceed to stage 2. The arrows that link the technological, organizational and environmental factors show that the factors influence one another. The arrows that link stage 2 and 3 shows that the technological, organizational and environmental factors impact CC readiness and vice versa.

B. *Technology Factors*

The technological factors include cost, ICT infrastructure, CC architecture, security, SLA, customization, dependence on internet, technology bottlenecks, data lock-in, lack of flexibility of user interface, integration issues, implementation issues, risk assessment and governance. They should first be considered in order to check the organization's capabilities in terms of the technological requirements of CC.

The cost of CC is the first factor that needs to be considered as it will be a waste of time to continue analysis if the organization cannot afford CC. The organization needs to make provisions for all the necessary infrastructure and architecture that will ensure there is continuous service availability in the cloud and the service, data, and infrastructure are available to authorized users immediately upon request [2]. The organization also needs to make plans to configure strong access control and API infrastructures that will improve security, integrity and data confidentiality. This will ensure that confidential and sensitive organizational data are not lost or exposed to unauthorized third parties once in the cloud.

The organization should also determine if there would be any need for customization of any of their applications or software in the cloud to meet their specific business requirements. This will help them in choosing a service provider that offers such level of customization. Since CC relies on the internet for its services, the quality of internet service is a vital requirement for CC as poor quality of internet service will result in poor quality of CC services. The organization needs to investigate the kind of internet services available to them and determine whether the quality of the available internet service meets the requirements of their CC service. All other known issues related to technology should be considered at this stage and proper plans should be put in place to provide solutions to them.

The issue of data lock-in should also be considered as it will give the organization the chance to negotiate with service provider from the start. This will also help resolve integration issues. Another important factor is lack of flexibility of user interface. The organization should include this in the criteria to select service provider. Implementation issues should also be dealt with so as to find ways to resolve them if and when they arise. Risk assessment and governance are also important because organization's need to understand the perceived risks involved with CC and how to mitigate them.

C. Organisational Factors

Organizational factors such as technology awareness, satisfaction with existing system, top management support, size of the IT resources, the utilization pattern of the resources, sensitivity of the data they are handling, criticality of work done by the company, skills, training, decrease in job satisfaction, lack of supporting resources, strategy issues, change management, malicious insider and risk management should be considered at this stage.

The organization needs to know about CC and related technologies so as to determine how it will fit into their business processes. The organization also needs to look at the existing systems in terms of cost, ease of use, efficiency and effectiveness and compare this with CC to determine if CC offers more benefit than the existing systems. The support of the top management is another important organizational factor as most organizations fail in their technology adoptions because there is no support from the top management. The size of the IT resources is also important at this stage because it will assist in selecting the right type of cloud. If the organization is a small organization, it may be cost effective to go for a public cloud as the data center and all other infrastructure will be provided by the service provider. If the organization is a large organization with large data center, choosing a private cloud may be the best option for them because they already have their data center and this will also give them control over their cloud infrastructure and ensure that security and privacy is improved. The utilization pattern of resources is also important because organizations that utilize a large amount of resources should be able to use that to negotiate for lower price with the service provider. This will assist them in cutting cost in the long run.

The sensitivity of data is also an important consideration at this stage. This will assist the organization to identify the more sensitive data and separate them from the less sensitive data. They will then be able to determine which ones to move into the cloud and which ones should remain in-house. The less sensitive data can be moved first into the cloud in order to test the cloud to see if it meets the organizational requirements. This will reduce the risks of data loss and other risks associated with moving into the cloud. The criticality of work done by the company should also be considered at this stage because stringent SLAs, resources, platforms, applications and security are needed for highly critical works while requirements of less critical works may be flexible.

Another important consideration at this stage is skills. There are some skills important for successful adoption of CC. The organization should arrange training for their IT staffs in order to equip them with the necessary skills for CC implementation. This will ensure that the staffs are able to tackle any issues that arise in a professional manner and avoid any problems that could have occurred as a result of lack of necessary skills. The possible impact of CC adoption on employees' job satisfaction should also be considered. It should be identified and necessary plans should be put in place to reduce such impact and improve employees job satisfaction as the success of adoption will be affected if employees' are not satisfied with their jobs as a result of changes from CC adoption.

Resources needed to support CC should be made available as this will ensure that CC runs smoothly. The organization also needs to develop CC strategies that will guide them during and after implementation. Another important factor the organization needs to consider is change management as CC will bring about change in their business. Risk management strategy should also be developed in order to reduce the risks identified. The possibility of having a malicious insider should also be considered and appropriate plans should be made to reduce possible risks as a result of malicious insider.

D. Environment

The environmental issues include cost, service provider, government support in terms of national infrastructure, regulations, legislation and jurisdictional issues, lack of standardized SLAs, competition from rivals and reputation fate sharing should be considered at this stage.

The cost of CC depends on environmental factors such as availability of service providers and availability of national infrastructure. The organization needs to investigate these factors at this stage to determine their impact on cost as they may drive cost high if their availability is low in the environment in which the organization is located. For example, if the availability of bandwidth is low, it will lead to an increase in the cost of CC. If service providers are also few in the environment, competition will be reduced and cost of CC will also be high. As noted by one consultant, the government support for CC in SA is inadequate and this will in one way or the other affect the CC readiness of organizations in SA.

The organization also need to carefully select a service provider by looking at the reputation of the service provider, the types of cloud services offered, functionality, ease of deployment, ease of upgrade and changes, SLA, costs, reliability and security. It is also necessary to verify the trustworthiness of a cloud provider by looking at the track record of the cloud provider in the market, number of clients in the financial industry or vertical, recommendations by research organizations, transparency shown during the due diligence, access to audit reports conducted by a third party and ability to provide evidence of controls and procedures. The ease of moving to another cloud provider and the ease of integration with in-house application and infrastructures should also be considered.

Regulations, legislations and jurisdictional issues should also be considered at this stage because they will have an impact on the success of CC adoption. For example, the cloud provider may have their data center in another location with different laws, regulations and legislations. The organization need to know which laws will be applied in this case and how that laws will affect them in terms of who owns the data, which laws, regulations and legislations are applicable etc. In SA, laws such as Protection of Personal Information (POPI) bill, Electronics Communications Act (ECA), Promotion of Access to Information Act (PIA), Financial Intelligence Centre Act (FICA) and Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) will help guide CC implementation.

VII. Summary and Conclusion

This paper proposes the BCCR framework which is a CC readiness assessment framework for organizations. It was developed for the financial sector but may, mutatis mutandis, prove to be useful for other organizations as well. The “Becoming Cloud Computing Ready” (BCCR) framework was developed based on the outcomes of the literature review, the TOE framework, the methods for managing change by [18] and many in-depth interviews with decision makers and consultants in the financial services industry in SA. Where the country characteristics of SA resemble those of other countries, particularly perhaps those of the Brazil, Russia, India, China, and South Africa (BRICS) countries, the framework may also be useful elsewhere.

The BCCR framework will assist (financial) institutions not only in determining whether or not they are ready for CC adoption, but to also identify how to improve their readiness level. It will also assist them to manage all the changes as a result of CC effectively. Overall, it is hoped that the BCCR will not only increase the chances of success of CC adoption but also help financial institutions reap the benefits of CC.

Limitations are the regional (South African) and industry (Financial Sector) contexts. Thus generalization to other contexts may not be possible. Future research should focus on the validation and extension of the framework, both by financial institutions and other organizations.

Acknowledgment

The first author would like to thank God for successful completion of this work. The authors would also like to thank Chief and Mrs Oladapo Akande for their continuous support. Finally, the authors would like to thank the National Research Foundation of South Africa (NRF) for their support which has made this work a success.

References

[1] E. D. Canedo, R. T. de Sousa Junior and R. de Oliveira, "Trust model for reliable file exchange in Cloud Computing," International Journal of Computer Science & Information Technology (IJCSIT), vol. 4, no. 1, pp. 1 - 18, 2012.

[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 1, pp. 583 - 592, 2012.

[3] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Services and Applications, 2010, 1 (1), 7 - 18.

[4] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The Characteristics of Cloud Computing", Proc 39th International Conference on Parallel Processing Workshops (pp. 275 - 279). Las Vegas: IEEE Computer Society, 2010.

[5] W.T. Tsai, X. Sun and J. Balasooriya, "Service-Oriented Cloud Computing Architecture", Proc 7th International Conference on Information Technology (pp. 684 - 689). Arizona: IEEE Computer Society, 2010.

[6] A. Goldstuck, "Corporate South Africa looks to the cloud for IT services," 16 November 2011. [Online]. Available: http://www.ipexpo.co.za/Highlights/Corporate-South-Africa-looks-tothe-cloud-for-IT-services. [Accessed 4 July 2012].

[7] H. Howell-Barber, J. Lawler, S. Desai and A. Joseph, "A Study of Cloud Computing Software-as-a-Service (SaaS) in Financial Firms", Journal of Information Systems Applied Research, 2013, 4 - 13.

[8] A. Sharma, "Data Management and Deployment of Cloud Applications in Financial Institutions and its Adoption Challenges," International Journal of Scientific & Technology Research, vol. 1, no. 1, pp. 1 - 7, 2012.

[9] A. Agopyan, E. Sener and A. Beklen, "Financial Business Cloud for High-Frequency Trading," in Proc 1st Int. Conference on Cloud Computing, GRIDs, and Virtualization, Lisbon, Portugal, Nov. 21 - 26, 2010.

[10] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges," in 24th IEEE Int. Conference on Advanced Information Networking and Applications, Perth, Australia, 20 - 23 April, 2010.

[11] V. K. Chauhan, K. Bansal and P. Alappanavar, "Exposing cloud computing as a failure," International Journal of Engineering Science and Technology, vol. 4, no. 4, pp. 1320 - 1326, 2012.

[12] S. C. Misra and A. Mondal, "Identification of a company’s suitability for the adoption of cloud computing and modelling its corresponding Return on Investment," Mathematical and Computer Modelling, vol. 53, no. 1, pp. 504 - 521, 2011.

[13] B. Hay, K. Nance and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing," in Proceedings of the 44th

Hawaii International Conference on System Sciences, Kauai, Hawaii, January 4 - 7, 2011.

[13] L.G. Tornatzky, F. Mitchell and A.K. Chakrabarti, "The processes of technological innovation", Massachusetts: Lexington Books, 2010.

[14] N. Kshetri, "Cloud Computing in Developing Economies: Drivers, effects and policy measures," in Pacific Telecommunications Council, Honolulu, Hawaii, January 17 - 20, 2010.

[15] U. Nasir and M. Niazi, "Cloud Computing Adoption Assessment Model (CAAM)," in Profes, Torre Canne (BR), Italy, June 20 - 22, 2011.

[16] A.O. Akande, N.A. April and J.P. Van Belle. "Management Issues with Cloud Computing," in Second International Conference on Innovative Computing and Cloud Computing, Wuhan, China, Dec 1 - 2, 2013.

[17] A.O. Akande and J.P. Van Belle. "Towards the Development of a Framework to Increase the Cloud Computing Readiness of Financial Institutions in South Africa," in Ochara, N.M. (2013) Proceedings of the 2013 International Conference on E-Leadership, Pretoria, South Africa, Nov 4 - 6, 2013.

[18] J.P. Kotter and L.A. Schlesinger, "Choosing Strategies for Change", Havard Business Review, 2008, 86 (7), 130 - 138.

[19] J. Attride-Stirling, "Thematic networks: an analytic tool for qualitative research", Qualitative Research, 2001, 1 (3), 385 - 405.

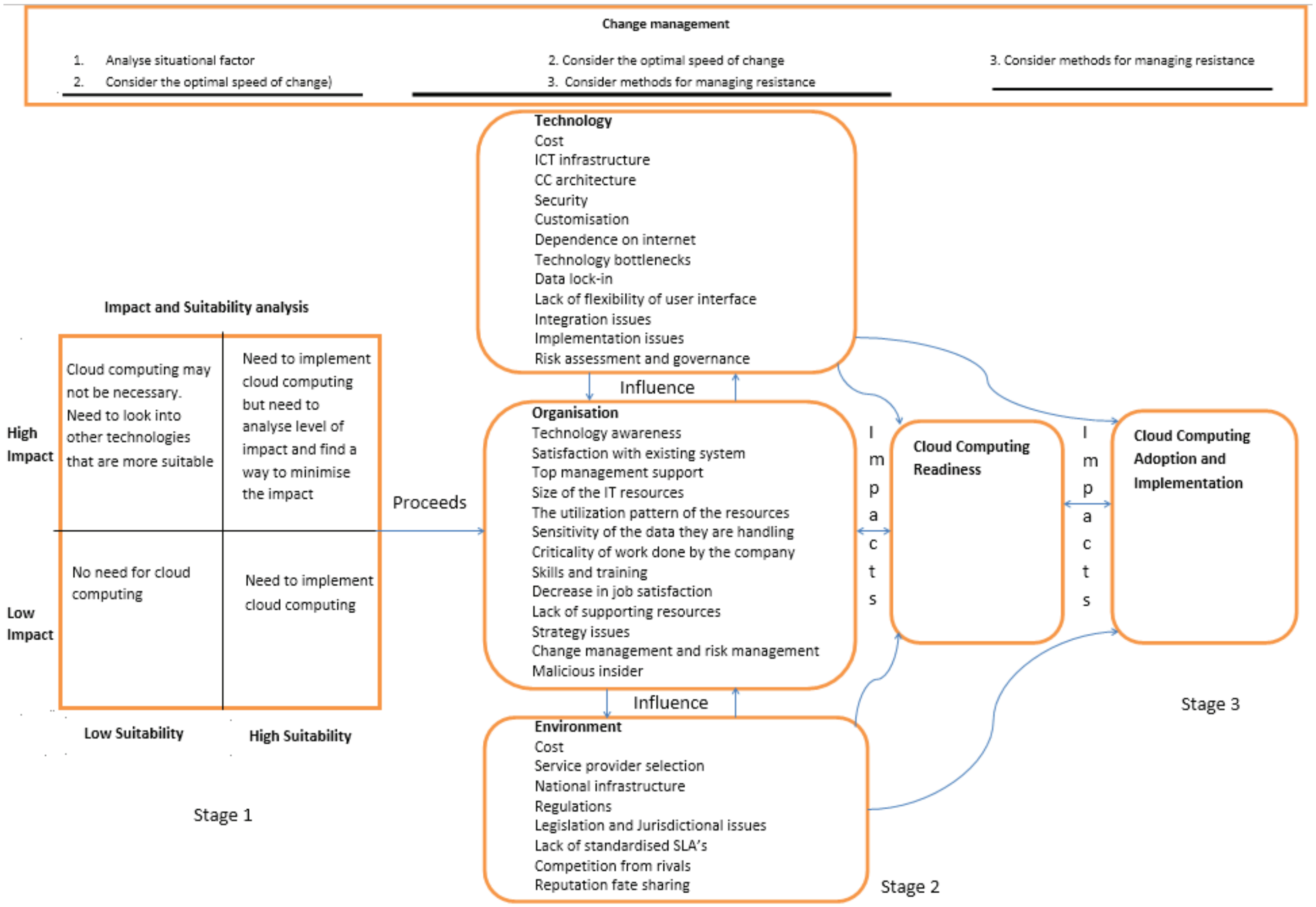
Change management
1. Analyse situational factor
2. Consider the optimal speed of change)
2. Consider the optimal speed of change
3. Consider methods for managing resistance
3. Consider methods for managing resistance
Impact and Suitability analysis
High Impact
Cloud computing may not be necessary. Need to look into other technologies that are more suitable
Need to implement cloud computing but need to analyse level of impact and find a way to minimise the impact
Low Impact
No need for cloud computing
Need to implement cloud computing
Low Suitability
High Suitability
Stage 1
Proceeds
Technology
Cost
ICT infrastructure
CC architecture
Security
Customisation
Dependence on internet
Technology bottlenecks
Data lock-in
Lack of flexibility of user interface
Integration issues
Implementation issues
Risk assessment and governance
Influence
Organisation
Technology awareness
Satisfaction with existing system
Top management support
Size of the IT resources
The utilization pattern of the resources
Sensitivity of the data they are handling
Criticality of work done by the company
Skills and training
Decrease in job satisfaction
Lack of supporting resources
Strategy issues
Change management and risk management
Malicious insider
Influence
Environment
Cost
Service provider selection
National infrastructure
Regulations
Legislation and Jurisdictional issues
Lack of standardised SLA's
Competition from rivals
Reputation fate sharing
Stage 2
Impacts
Cloud Computing Readiness
Impacts
Cloud Computing Adoption and Implementation
Stage 3

Fig. 1. The proposed "Becoming Cloud-Computing Ready" Framework for financial institutions