Article

Migration of Applications and Information Systems to Cloud Computing Infrastructure: Lessons from a South African Retail Bank

Rabelani Dagada
https://orcid.org/0000-0002-3025-6678
University of South Africa
dagadr@unisa.ac.za

Abstract

The aim of this study was to investigate the benefits and challenges of moving information systems to the cloud infrastructure as part of phasing out legacy systems and preventing digital fraud. This study employed a qualitative research methodology and used interviews, observations and document analysis as data-collection methods. It was confined to one bank and is therefore classified as a case study. To protect the identity of this organisation, the researcher gave it a pseudonym called SA Retail Bank. The study yielded three major findings. Migration of applications to a cloud environment is characterised by several unexpected technical, regulatory and people challenges. However, the migration yields operational benefits such as reducing fraud, quick recovering of stolen moneys, and advancing Fourth Industrial Revolution technologies. Technology acceptance theories should also be prioritised to get the support of both internal users and customers. The findings of this study present important lessons for digital businesses in South Africa and abroad. The research yielded theoretical and practical contributions. Recommendations were also made for future research.

Keywords: legacy information systems; data migration; cloud computing infrastructure; information systems strategy; technology acceptance theories

UNISA university of south africa PRESS
Mousaion: South African Journal of Information Studies
#16035 | 18 pages
https://doi.org/10.25159/2663-569X/16035
ISSN 2663-659X (Online)

Introduction

Bandari (2022) claims that banks have been hesitant to abandon legacy information systems either because they are still functioning or because change can be difficult. However, it is no longer possible to stop a wave of migration to the cloud environment. In addition, the advantages of cloud computing outweigh those of legacy information systems by far.

In the South African retail bank sector, artificial intelligence is used to improve customer experience and engagement, identify exceptions and irregularities, increase revenues, reduce the expenses, find predictability in the patterns, and increase forecasting dependability. SA Retail Bank has been in the process of improving its operations, phasing out legacy information systems, and migrating its modernised information systems and applications to the cloud computing infrastructure.

The migration process was being incrementally to avoid massive banking disruption. Fraud detection and transactional banking applications were the first to be migrated to the cloud. The slow migration of all SA Retail Bank's applications has been affecting engineering and technology departments as well as customers' experiences and revenue generation.

According to Alharthi (2023), cloud computing has become one of the major developments of information systems in recent years. Cloud services enable users to access applications and data on demand, wherever they are and whenever they need it. SA Retail Bank has been investing in cloud infrastructure. Its management believed it would place the bank in a more desirable position to service its customers better and increase its market share.

Cloud migration projects focus on improving operations that are being throttled by legacy information systems (Kunduru 2023). Cloud computing is service-oriented and it enhances digital banking. According to Shaikh and Anwar (2023), digital banking focuses on ensuring that permissions are followed properly and informs customers that SA Retail Bank is using their data to perform better services. This creates a personal relationship between SA Retail Bank and most of its customers. Challenges that customers encounter can be resolved using data instead of assumptions. The bank had intended to embark on a process to enhance its information systems and applications to provide "always-on" activities.

Migrating information systems and applications to cloud computing infrastructure is part of business innovation and digital transformation. Bogoviz and Ragulina (2020) define business innovation as a process to reduce various kinds of risk while boosting service reliability and quality through a systematic approach.

Hosting services in the cloud infrastructure lead to low inter-failure correlation, low hardware costs, high efficiency factors, and low levels of fraudulent activities and other

types of cyberattack (Kunduru 2023). Dagada (2013) defines fraud as the activity of deliberate misinformation or dishonesty committed by one or more people, usually for personal monetary benefit. It is important for the organisation to implement proper measures to prevent fraud, fast-track investigations, and detect the gaps within its applications and information systems.

These terminologies – cloud, cloud services, cloud infrastructure, cloud environment and cloud computing infrastructure – are used interchangeably in this study and carry the same meaning.

Research Context

Shaikh and Anwar (2023) assert that banks should use a tiered approach to stay up to date with escalating cyberattacks and fraudulent techniques because fraudsters are always looking for loopholes. Cloud migration provides an option for the digital businesses and their employees to exchange data immediately, synchronise folders, share access and take necessary steps if needs be.

The board of directors and executive committee (Exco) of the SA Retail Bank took the decision to invest in cloud computing after studying a business case prepared by heads of business units in SA Retail Bank. They reasoned that migration would enable the bank to accomplish its vision of transforming from a typical bricks-and-mortar firm to being an agile digital business.

Before migration, fraud detection and transactional banking applications were hosted in various on-premises legacy information systems. It was tedious for cybersecurity practitioners to gather data from these disparate information systems to either prevent or investigate fraudulent activities. The Exco mandated the chief information officer (CIO) to serve as the project manager for migrating all SA Retail Bank applications and information systems to the cloud computing infrastructure.

The Exco was convinced that the migration to the cloud would enable SA Retail Bank to tighten its cybersecurity. In addition, cloud computing offered the flexibility to test new services and solutions in one business unit and quickly scale them across the whole organisation. This factor was extremely important for SA Retail Bank, with its large size and scope. SA Retail Bank could develop new services using the advanced technologies to satisfy shifting customers' needs and quickly deliver customised products in response to fierce competition in the sector. Like many other banks in South Africa, SA Retail Bank appointed Amazon Web Services (AWS) to host its data in the cloud.

SA Retail Bank has three strategic priorities that underpin everything it does, namely, narrowing its focus and increasing the likelihood of swift and impactful execution, transforming customers' experiences by striving to understand their needs as deeply and

empathetically as possible, and employing digitalisation to meet their needs. It was important for SA Retail Bank to have a stable environment and efficient technology to achieve all its goals and objectives. The bank executives believed that cloud computing would contribute towards the achievement of its strategic objectives.

Research Problem

Digital banking customers are tricked by cybercriminals using techniques such as phishing and vishing (voice phishing), getting them to download Trojan horses and other harmful software which can provide the criminals with access to their login information (Dagada 2021). Even after being warned by banks about various methods that fraudsters use to obtain access to their banking accounts, customers continue to become victims of cybercrime.

The number of daily digital fraud cases has increased, and investigators who rely on data which is hosted in on-premises legacy information systems must work through backlogs before they can close each case (Alharthi 2023). Before deciding whether a case involves fraud or not, digital fraud investigators should have all the facts available to them and should attach all the evidence to the case before taking further steps. Cybercriminals continue to search for possibilities of digital banking to further their malicious goals of financial gains by hacking the networks (Dagada 2013, 2021).

The global banking system's stability is becoming increasingly affected by cybercrime (Shaikh and Anwar 2023). It is therefore crucial and challenging to ensure that highly robust information systems are in place to protect sensitive data as banks become more digitalised and rapidly gather larger amounts of data. A significant rise in cyberattacks has become a major concern to customers, banking sector executives, regulators and policymakers. The most frequent bank scams involve credit cards, money laundering, international theft, online banking, sending fraudulent emails and misrepresenting clients (Dagada 2021).

An extensive search in scholarly databases found that no single study had ever been published which focused on the migration of applications and information systems to the cloud computing infrastructure in the South African banking sector, and the ways in which this would affect fraud detection and transactional banking. This study was undertaken to attempt to close this gap in information science literature.

The Aim of the Study

The aim of this study was to assess the intricacies of phasing out legacy information systems, and preventing and enhancing digital fraud investigations by migrating fraud detection and transitional banking applications from on-premises data centres to be hosted in the cloud computing infrastructure.

The research question was as follows: How can migration of banking applications and information systems to the cloud computing infrastructure enhance fraud detection and transactional banking?

Challenges of Migrating to the Cloud

The literature shows that many organisations, which migrated their information systems from on-premises data centres to be hosted in the cloud, have experienced several challenges (Alharthi 2023; Saidi and Bardou 2023). Occasionally, information systems managers find that there are applications that perform less optimally in the cloud environment than they did on-premises. Other concerns include insufficient latency, security concerns, lack of skilled personnel and compliance issues. The migration project manager needs to think about where the data will go, how to handle the technical transfer, and how to resolve any potential commercial or legal problems.

Underestimating the importance of proper employee training is a fatal mistake (Saidi and Bardou 2023; Stephanou and Dagada 2008). It takes a different set of management skills to manage applications and information systems in the cloud environment, as opposed to managing them on-premises. Making sure that everyone is adequately trained on how to manage the relevant services should be a priority for the engineering department, which should also consider the skills sets of the employees.

If employees' training cannot be completed in advance of a cloud migration, contractors from vendors might be employed to work on the project while the team is undergoing training (Alharthi 2023).

Cloud migration, as mentioned by Jangjou and Sohrabi (2022), is a significant undertaking and can be intimidating. The project team can start small, think big and act quickly. A set of direct leads that enable a longer-term solution should be included in the first migration effort, which will be a valuable learning experience. In addition, it should assist in identifying any talent gaps and prospective partnerships with vendors that could contribute significantly to the wider cloud migration plan (Mangalagowri and Venkataraman 2023).

Benefits of Cloud Computing

The benefits of migration far supersede the inconvenience of transitioning millions of banking customer accounts and thousands of software processes to an entirely new environment (Bandari 2022). While companies have been concerned about the security of cloud computing infrastructure, it is becoming increasingly difficult to ignore its benefits.

As mainframe information systems get older, so does the number of technical experts who are familiar with them (Hasan et al. 2023). The remaining software engineers and other technical experts who are running legacy information systems are mostly white males in their late 50s, 60s and 70s (Dagada 2024).

Evidence generated by industry case studies and academic research has convinced banking executives that cloud services provides far better cybersecurity than the information systems. Financial services sector regulators are increasingly viewing decades-old core information systems as a potential business risk (Dagada 2021).

The main justification given by organisations about transitioning to a cloud environment is to reduce the costs of replacing the on-premises infrastructure and refocusing back-end software developers to support the front-end software development activities (Hasan et al. 2023). Cloud computing is superior in the protection of data confidentiality, integrity and availability. It enables information systems and applications to operate more quickly and be more flexible. It also provides high levels of disaster recovery and business continuity (Kunduru 2023).

According to Dagada (2024), digitalisation is driving our new way of life, with radical changes in the way we feel, expect, behave, perceive emotions, express passions and behave sentimentally. Victims of digital fraud expect feedback from banks swiftly, and to be notified of unusual activities in their accounts. Cloud computing is highly beneficial in this regard.

Lanza (2022) states that banks require a bold vision and a workable execution strategy to accelerate their move to the cloud environment. Organisations should not view going to the cloud as an end in itself, but rather as a continuous business improvement process. A well project-managed migration can come in handy in uniting a company behind one major milestone. It can serve as a motivator for effectiveness, innovation and expansion (Alharthi 2023). The organisation should modernise its processes and customer services once it has moved a sizable portion of its workload into the cloud environment because it can then quickly recover the expenses.

Research Methodology

It has already been mentioned that this study adopted a case study approach. This should be attributed to the fact that SA Retail Bank was the only bank among the five dominant retail banks in South Africa that agreed to participate in this study. Merriam (1998) differentiates case studies from generic studies on the grounds that the former lend themselves to intensive description and analysis of a bounded system such as a programme, a person or a community.

Research Design

This study employed the qualitative research methodology in a case study. The reason for using the qualitative approach was that the respondents could constitute a rich and valuable source of information (Kenny et al. 2023). This study went "beyond numbers" and statistics (Greenhalgh and Taylor 1997, 741). It took the form of a case study to examine issues and challenges pertaining to SA Retail Bank's migration of banking systems and applications to the cloud computing infrastructure.

Sampling and Research Participants

Purposive sampling was used to select the participants for this study. The participants were deliberately chosen because the jobs they occupy in the SA Retail Bank would enable them to provide information which would answer the research question. A sample of 10 research participants from SA Retail Bank's management and engineering teams participated in the study.

To strengthen the findings and the validity of the study, the researcher also interviewed five professionals outside of SA Retail Bank, as follows: a professor of information systems management based in a postgraduate business school, a managing executive of digital banking channels, a head of virtual channels based in a bank, a head of enterprise information architecture based in a hotel group, and a team leader of application development based in a mobile network operator.

Data-Collection Techniques

The study used qualitative data-collection methods. This study complied with the principle of triangulation by using multiple data-gathering methods and sources (Shrivastava and Shrivastava 2023). The data-gathering methods in this study were interviews, observation and document collection and analysis thereof.

Semi-structured interviews were used to conduct 15 individual interviews. These interviews made it possible for the researcher to obtain information from the interviewees. The interview is a particularly suitable data-gathering method for the environment concerned and made it possible to collect valuable information with reference to the type of research question. This provided the researcher with an opportunity for direct exchange with the participants of the study, and to get hold of the facts directly from them.

The study employed observation as one of the data-collection methods. This enabled the researcher to observe the impact of cloud computing infrastructure on SA Retail Bank's fraud detection and transactional banking applications. The researcher observed and tested the functionality of applications. He did this as a bank customer instead of being an information systems specialist. This is important because what matters most is the user experience (Dagada 2021).

Grabs and Carodenuto (2021) declare that observation as a data-collection method has several advantages over interviews. The researcher's attitude is that both observations and interviews complemented each other in this study. They also enriched its findings. During the observation, the researcher took notes. It was on this premise that written permission was sought and obtained from SA Retail Bank.

Documents containing the business case for migrating SA Retail Bank's applications and information systems to the cloud computing infrastructure and the technical requirements for doing this were collected from the CIO, reflected upon and analysed.

The data from the interviews, observation notes and the document analysis were evaluated against the literature dealing with the migration of information systems and applications to the cloud computing infrastructure. These data were used to answer the research question.

Data Analysis

The data gained from the interviews were analysed using open coding (Li and Zhang 2022). A recurrent comparative method was applied to analyse the data during and between the interviews. Content analysis was also applied to analyse the content of the interviews (Merriam 1998). The process entailed the instantaneous coding of raw data and the formation of categories.

The data were analysed with the objective to discern common patterns and to put together categories. These were weighed against the literature. These categories were used to answer the research question.

The data collected through document analysis and observation notes were analysed by matching it with the data collected from the interviews, and through content analysis.

Research Ethics

Ethical aspects were observed in this research even though it carried low risk. The research participants were requested to participate in this study. The requests were delivered through email. All research participants agreed to take part in this study by providing written approval.

All interviewees agreed to the recording of discussions during the data gathering. The researcher coded the audio-recorded conversations and stored the recordings in a password-protected computer and a locked facility.

The participants were at liberty to withdraw from the study at any time without being required to give reasons. All necessary measures were taken to guarantee that persons taking part in the study were not caused any harm by participating. For that reason pseudonyms were used to protect the identity of the participants and to make sure that

any information, either personal or professional, that was revealed during the interview was handled as confidential.

Ethical clearance was obtained from the Faculty of Humanities Research Ethics Committee at the University of Johannesburg.

Findings of the Study

This study generated the following three major findings: (1) migration of applications to cloud computing infrastructure is characterised by several challenges related to technology, regulatory and people challenges; (2) migration to cloud computing infrastructure has reduced digital fraud; and (3) critical factors to consider when migrating to cloud computing infrastructure.

Finding 1: Migration of Applications to Cloud Computing Infrastructure is Characterised with Several Technical, Regulatory and People Challenges

During the interview process, the participants were asked to identify and explain the challenges associated with the migration of banking applications and information systems to the cloud environment. The participants provided various responses. The engineers indicated that they were extra careful when migrating fraud and transactions applications because their security is crucial. This made the migration process delicate and slower than expected.

The provisions of the Protection of Personal Information Act of 2013 were also adhered to as part of the migration to the cloud. “We had to create some new features suitable for the new environment and this has impact to the user experiences. This required lot of change management to stakeholders and customers who were part of the pilot process” (Interviewee A).

While this project had the support of the bank’s Exco, there were times that the project team “experienced some pushback from the executives” (Interviewee B). Getting support from the business is a particularly difficult problem with being afraid of the unknown.

SA Retail Bank had hundreds of legacy information systems which hosted important applications. Moving applications from legacy information systems to SAP (an enterprise resource planning system) and then migrating it to the cloud computing infrastructure were highly complicated. This was exacerbated by the scale of the organisation and the volume of the data.

The analysis shows that there were several challenges faced by the SA Retail Bank employees when migrating SA Retail Banking applications and information systems to the cloud computing infrastructure because the legacy information systems, SAP and

the cloud infrastructure “did not talk to each other” (Interviewee C). These findings support those of Alharthi (2023), who claims that banks have been hesitant to abandon legacy technology because the migration to the cloud was a daunting task.

SA Retail Bank has been trying to migrate applications housed in legacy information systems to SAP with limited success. This had become urgent because most software engineers who have the expertise to run these applications are approaching retirement. In addition, young software engineers are not interested in old technologies. Most importantly, the organisation had taken the decision to start by migrating its fraud and transactional banking applications to the cloud computing infrastructure. Other applications would be migrated later.

The study found that it could be challenging to foresee how the migration of applications into the cloud infrastructure will work out. The cloud itself provides some enormous capabilities that can be maximised to benefit customers. Ideally, SA Retail Bank should at once move all its applications to the cloud computing infrastructure, but this was not practical and possible businesswise. Still, migrating application bit by bit also posed challenges. Some of the applications that were already on the cloud “had to talk to the applications that were sitting on-premises” (Interviewee D).

The on-premises applications are slow by nature, and they also present other complications, so there is a difficulty regarding latency and efficiency, since a specific application would now be comparing the two systems. “Engineers had to find a way of combining the two systems and this requires a lot retrofitting” (Interviewee B).

The cloud computing infrastructure also requires new skills sets. Because of the shortage of skilled engineers and technical support staff, internal users are sometimes compelled to continue using applications that are on-premises. On the other hand, the performance of the applications in the cloud that are not fully engaged tends to suffer. Staff that relocated to manage applications in the cloud computing infrastructure needed to be upskilled urgently.

The biggest challenge that the engineering team faced was to get permission from the Exco to migrate more applications to the cloud. The executives wanted to be convinced that there was a proper level of security to protect that data before granting this permission.

This study found that migration to the cloud computing infrastructure required specific architecture. This consists of three categories of information sources for achieving business agility, namely, availability, collaboration and elasticity. This included deployment and the use of a cloud service which comprised software, information and reliable infrastructure. Configuring the architecture, interface and back-end properly proved to be difficult.

During the regular engagements between the CIO and the Exco, data security and governance were the other issues that were mostly raised by the executives. The engineers had to convince the executives that when they migrate and store data in the cloud computing infrastructure, they would abide by certain banking regulations and technical standards.

The executives did not want a situation where the migration of systems disrupted applications that are regularly used by the customers. Other than causing inconvenience, this may lead to reputational risks and some customers may migrate to other banks. “That is why we did the actual physical migrations technical between 9 pm and 6 am. Each time we did this, SA Retail Bank would warn customers” (Interviewee C).

This study found that the cloud computing infrastructure has minimum industry security standards. This should be attributed to the fact that, compared to the traditional data centres, “cloud computing is relatively new” (Interviewee E).

The engineers of SA Retail Bank and their counterparts at the cloud infrastructure company had to devise their own standards and technical measures to tighten cybersecurity. This made cloud infrastructure to meet a defined high level of security standards. “Executives were concerned that the cloud environment was hosted outside of the control of the bank-owned data centres” (Interviewee D). Cloud computing data centres are generally managed by cloud infrastructure providers such as AWS, Microsoft, Oracle, Google or Azure.

According to Mangalagowri and Venkataraman (2023), the organisation should be ready to restructure governance workflows and alignments, because in the cloud they are required to be more agile and continuous, with various technical disciplines. This requires quicker decision-making than normal for on-premises governance methods.

Finding 2: Migration to Cloud Computing Infrastructure Has Reduced Digital Fraud

As part of migration, SA Retail Bank has introduced additional layer identity authentication when one logs into online banking. This has substantially reduced digital banking fraudulent activities. Because cloud environment is agile and provides real-time data, cybersecurity practitioners can stop fraudulent activities quickly.

“Investigations are also done quickly after the incidents, and it is much easier to trace the digital footprints of the fraudsters” (Interviewee F). Customers also receive real-time alerts when SA Retail Bank becomes suspicious of fraud taking place. This has improved the recovery of those fraudulent transactions. When the bank still had its fraud and transactional banking applications in the on-premises environment, it would take cybersecurity practitioners hours before they sent alerts to defrauded customers. “Unfortunately, by then the horse would have already bolted and recoveries were excessively difficult” (Interviewee B).

Systems that have been migrated to the cloud computing infrastructure provide a clear picture of each account to cybersecurity applications. For example, a cybersecurity practitioner can see all the subaccounts that are legitimately connected to the main account, and this makes it easy to detect unusual and fraudulent activities. “The on-premises environment did not provide this cybersecurity efficiency” (Interviewee G).

However, it should be emphasised that information systems in general and cloud computing in particular are not the panacea for all our cybersecurity challenges. Human beings are the weakest link when it comes to security (Dagada 2013). For the migration to cloud to achieve its full potential, people, skills and culture have to change and that has not yet been sufficiently achieved. “It is work in progress” (Interviewee E).

Cybersecurity practitioners and fraud detection applications “are fire extinguishers in the bank; especially when one considers the escalating cyberattacks in South Africa” (Interviewee H). The migration to cloud computing infrastructure has brought with it many cybersecurity advantages because it has converged advanced technologies that were traditionally stand-alone and distinct, such as artificial intelligence, big data, the internet of things and sensors. This is important in curbing fraudulent activities. “Truly speaking, while cloud computing is considered not to have matured industry security standards, it has more cybersecurity advantages than on-premises data centres” (Interviewee I).

Another advantage of cloud computing is that it has enhanced machine learning. Systems use the collected data to learn and improve themselves in real time. “Machine learning capabilities can be run on that data to provide the security team and customers with instant red flags, certain alerts, or certain trends that they could not pick up in a traditional data centre set-up” (Interviewee J).

The success of migrating fraud and transactional banking applications to the cloud has encouraged other functions to either “start embarking or speeding-up their migrations journeys” (Interviewee E). It has also made the job of the CIO easier in his dealings with the Exco. The chief executive officer has now become an executive sponsor of migration to the cloud environment.

Finding 3: Critical Factors to Consider When Migrating Applications to Cloud Computing Infrastructure

The professor emphasised that an organisation’s information systems strategy is a major factor regarding the migration of data to the cloud. She asserted: “It should be borne in mind that the information systems strategy defines the organisation’s requirements for information and systems to support the overall strategy of the business”. Information systems strategy should be firmly grounded in the business, taking into consideration both the competitive impact and alignment of requirements of information systems.

The assertions of the professor were supported by the head of virtual channels, who said: “Essentially, information systems strategy defines and prioritises the investment required to achieve the ideal applications portfolio, the nature of the benefits within the constraints of resources and systems interdependencies”. An information systems strategy indicates how it would support the organisational strategy. If the information systems strategy does not do this, it would lack credibility and will not get the support of the board of directors, Exco and other stakeholders.

The decision to phase out legacy systems, and modernise, digitalise and move systems and applications from on-premises to the cloud computing infrastructure should emanate from both the organisational and information systems strategies. “If this is not the case, the entire migration project is bound to fail,” said the head of enterprise information architecture.

The head of enterprise information architecture further declared that: “A major concern emerging worldwide is that information systems has in more ways than one become disconnected from the business and is thus losing touch with the core activities of the business”.

When major organisations, both in the private and public sector, evolve and restructure, they tend to temporarily lose focus. This may result in support functions such as information systems assuming a corporate life of their own without necessarily being aligned with the core business of the organisation.

The managing executive of digital banking observed that: “In the process, information systems practitioners would implement projects like enterprise resource planning, digitalisation, advanced 4IR technologies, and cloud computing merely because they are current industry buzzwords”.

Information systems projects will not get executive support and funding if they are not rooted to the organisation’s strategy. This statement is supported by Diamandis and Kotler (2020), who alluded that directors’ and executives’ decision-making is largely influenced by competitiveness, growth, sustainability, bottom-line and value creation for the shareholders instead of the usual buzzwords.

The managing executive of digital banking channels advised that before an organisation embarks on a massive project such as migrating its systems and data to the cloud it should consider three factors – the global information systems environment, national information systems and regulatory trends, and internal dynamics.

The trade war between the United States and China has huge implications to the information systems subsector globally. The CIO and her team should reflect on the existing information systems-related research and case studies in Asia, emerging markets and developed economies. The uptake of mobile phones, smartphones, iPads

and tablets is growing rapidly in southern Africa, and this should be factored in the information systems strategy in general and the cloud migration project in particular.

The allocation of the high-demand spectrum to mobile network operators in South Africa and the increasing presence of the Starlink satellite internet connectivity in most southern African countries bodes well for the advancement of 4IR, growth of digital business, increased uptake of digital banking, and adoption of cloud computing in the region.

The head of virtual channels suggested that executives should pay attention to the national policies, legislation and regulations. For example, in South Africa, the Protection of Personal Information Act of 2013 has a big impact on the ways in which organisations should manage the collected data. Consequently, this would influence their cloud migration strategy. "The provision of public infrastructure should have a lot of impact both in the overall organisational and information systems strategy. This includes electricity, roads, rail, and broadband infrastructure".

The professor indicated that the CIO and her team should ask themselves these two questions: "Firstly – what are the individual and corporate customers' trends in terms of the information systems applications uptake in the country? Secondly – are we going to get relevant skills to deploy and support our cloud infrastructure?"

With regard to the internal organisational environment, the managing executives said that information systems management should pay attention to the following factors: the organisation's strategic plan, structure, policies, culture, business requirements and existing information systems infrastructure. Most information systems projects fail because the CIOs do not consider these organisational issues.

Information systems management should build a business case for each major project and get the support of the Exco before they start the project. The professor argued that information systems is no longer just a support function in digital businesses; it is both a delivery channel and a significant profit centre.

She continued:

> A typical board of directors would have the following subcommittees – nomination and governance; audit, safety, social and ethics; and renumeration. Digital businesses like Naspers, Meta Platforms, Amazon, Alphabet, Bank Zero, and Tyme Bank should have a standalone information systems subcommittee in their boards.

The head of virtual channels observed that the reason why information systems projects fail is that the Excos in most organisations relegate technology to the support function despite the fact that it consumes a huge amount of the capital budget, it is a delivery channel, and it handles delicate projects such as the implementation of enterprise resource planning and the migration of data to the cloud.

If companies want their data migration and other information system projects to succeed, they should establish a steering committee on information systems, which will be chaired by a senior executive at the level of the chief operations officer. The steering committee will monitor and assess information systems operations and projects. This committee should, among other things, include the heads of each business unit.

In addition, sub-steering committees should be established for each major information systems project. CIOs should use pilot projects before implementing fully-fledged projects. This will enable the team to identify major issues and gain important insights. They will also be able to celebrate small successes, which will encourage the information systems team and win over the support of the Exco.

The professor, managing executive of digital banking, head of virtual channels and senior cybersecurity advisor agreed that, while cloud computing enhances the performance and the convergence of artificial intelligence, generative artificial intelligence applications, big data, the internet of things, sensors and robotics, this has led to the escalation of digital fraud and other types of cyberattack.

They all agreed that cloud infrastructure makes it much more efficient and quicker to mitigate and fight against cyberattacks. They also concurred with the engineers whom the researcher interviewed at SA Retail Bank that cloud computing makes it easier to instantly stop digital fraud, and investigate and recover the stolen funds.

The team leader of applications development cautioned that gaining the support of the board and Exco is not sufficient to successfully migrate applications and data to the cloud computing infrastructure. Both internal users and customers should be taken on board by providing for these factors: change management initiatives, technology acceptance theories, perceived self-efficacy, perceived easy-of-use, perceived usefulness, perceived risk and credibility, users' convenience, and trialability. These are important lessons for digital business in southern Africa and other jurisdictions.

Contributions of the Study

A search in scholarly databases did not yield any results of previous studies that dealt with the migration of systems from on-premises data centres to cloud computing infrastructures in the South African banking sector. This study somewhat closes that literature gap, and it has contributed to the information science body of knowledge.

The study also offers various practical contributions. These include the importance of gaining the support of top management and other stakeholders. The findings of this study make it apparent that software developers and other technical engineers must be equipped with the necessary skills to migrate and manage applications in the cloud environment.

Limitations of the Study

Case studies have several weaknesses. More than 20 local and foreign banks operate in South Africa. The researcher is not totally convinced that the findings of this study are transferable to other banks in South Africa and southern Africa. The research participants could have been biased. However, this was mitigated by interviewing five experts who are based in other organisations. This enabled the researcher to test some of the pronouncements of SA Retail Bank's 10 employees who were interviewed for this study.

Even if these limitations are accepted, the study is still regarded as valuable to the information science body of knowledge; especially considering that this was a case study using a qualitative research approach.

The researcher had a strong understanding of the literature that had been published on the research topic and accurately assessed the assertions of the interviewees against the literature. The conclusions are therefore supported by credible data. This exploratory design was intended to lay the groundwork for future extensive research studies on this topic.

Concluding Remarks and Recommendations for Future Research

This article presented the research findings of and proposed solutions for the migration of banking applications and systems to the cloud environment to improve digital fraud detection and transactional banking applications. It was indicated that SA Retail Bank intends to eventually phase out all the legacy technology and migrate all its systems to the cloud to improve business efficiency and to increase its market share.

The study's limitations were described. Despite the shifting nature of the South African retail bank sector and digital business, it is recommended that organisations cater for the factors that influence the success of cloud migration and other major information systems-related projects.

The researcher further recommends that organisations assess their applications and systems periodically to ensure they are aligned with the advancing technologies and digital business rapid evolution. Organisations should continuously train their employees so that they can cope with rapid digitalisation of functions. Emphasis should also be put on technology integration of the labour force, and employees–technology coexistence (Dagada 2024).

The effectiveness of cloud computing as regards cybersecurity and other functions should become a regular item on the agenda of the information systems steering committee. This will enable management to gain insights and take the necessary steps if needs be. The outcome of this exploratory study supports the development of more

informed decisions on the issues involved with the SA Retail Bank's migration of banking applications and systems to cloud environments.

At the time of doing this study, SA Retail Bank had only migrated fraud and transactional banking applications to the cloud computing infrastructure. Future studies should focus on the retail banks operating in South Africa that have migrated almost all their functions to the cloud environment. Having noted the limitations of this study which emanated from the case study methodology, it is advisable to broaden future studies to include several organisations and also the use of a mixed-methods approach.

References

Alharthi, D. 2023. "Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud." *International Conference on Cyber Warfare and Security* 18 (1): 1–6. https://doi.org/10.34190/iccws.18.1.1038.

Bandari, V. 2022. "Optimising IT Modernisation Through Cloud Migration: Strategies for Secure, Efficient and Cost-Effective Transition." *Applied Research in Artificial Intelligence and Cloud Computing* 5 (1): 66–83.

Bogoviz, A. V., and Y. V. Ragulina (Eds.). 2020. *Industry Competitiveness: Digitalization, Management, and Integration*. Springer. https://doi.org/10.1007/978-3-030-40749-0.

Dagada, R. 2013. "Digital Banking Security, Risk and Credibility Concerns in South Africa." *Digital Banking Security* 10 (3): 148–49.

Dagada, R. 2021. *Digital Commerce Governance in the Era of Fourth Industrial Revolution in South Africa*. Unisa.

Dagada, R. 2024. "Will Employees and Technology Continue to Coexist Despite Historic Tensions? *African Journal of Employee Relations*. https://doi.org/10.25159/2664-3731/13466.

Diamandis, P. H., and S. Kotler. 2020. *The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives*. Simon and Schuster.

Grabs, J., and S. L. Carodenuto. 2021. "Traders as Sustainability Governance Actors in Global Food Supply Chains: A Research Agenda." *Business Strategy and the Environment* 30 (2): 1314–32. https://doi.org/10.1002/bse.2686.

Greenhalgh, T., and R. Taylor. 1997. "How to Read a Paper: Papers That Go Beyond Numbers (Qualitative Research)." *BMJ* 315 (7110): 740–3. https://doi.org/10.1136/bmj.315.7110.740.

Hasan, M. H., M. H. Osma, N. I. Admodisastro, and M. F. Muhammad. 2023. “Legacy Systems to Cloud Migration: A Review from the Architectural Perspective.” *Journal of Systems and Software*, 202: 111702. https://doi.org/10.1016/j.jss.2023.111702.

Jangjou, M., and M. K. Sohrabi. 2022. “A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing.” *Archives of Computational Methods in Engineering* 29 (6): 3587–608. https://doi.org/10.1007/s11831-022-09708-9.

Kenny, N., A. Doyle, and F. Horgan. 2023. “Transformation Inclusion: Differentiating Qualitative Research Methods to Support Participation for Individuals with Complex Communication or Cognitive Profiles.” *International Journal of Qualitative Methods* 22. https://doi.org/10.1177/16094069221146992.

Kunduru, A. R. 2023. “Artificial Intelligence Advantages in Cloud Fintech Application Security.” *Central Asian Journal of Mathematical Theory and Computer Science* 4 (8): 48–53. https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/492.

Lanza, N. “The Ultimate Guide to Banking in the Cloud.” *Accenture*, 18 July 2022, https://bankingblog.accenture.com/the-ultimate-guide-to-banking-in-the-Cloud.

Li, Y., and S. Zhang. 2022. “Qualitative Data Analysis.” *Applied Research Methods in Urban and Regional Planning* 149–65. https://doi.org/10.1007/978-3-030-93574-0_8.

Mangalagowri, R., and R. Venkataraman. 2023. “Ensure Secured Data Transmission During Virtual Machine Migration Over Cloud Computing Environment.” *International Journal of System Assurance Engineering and Management* 1–12. https://doi.org/10.1007/s13198-022-01834-8.

Merriam, B. S. 1998. *Qualitative Research and Case Study Applications in Education*. Jossey-Bass.

Saidi, K., and D. Bardou. 2023. “Task Scheduling and VM Placement to Resource Allocation in Cloud Computing: Challenges and Opportunities.” *Cluster Computing* 26 (5): 3069–87. https://doi.org/10.1007/s10586-023-04098-4.

Shaikh, I., and M. Anwar. 2023. “Digital Bank Transactions and Performance of the Indian Banking Sector.” *Applied Economics* 55 (8): 839–52. https://doi.org/10.1080/00036846.2022.2094880.

Shrivastava, S. R., and P. S. Shrivastava. 2023. “Data Collection Process in Qualitative Research: Challenges and Potential Solutions.” *Medical Journal of Dr.DY Patil Vidyapeeth* 16 (3): 443–5. https://doi.org/10.4103/mjdrdypu.mjdrdypu_871_21.

Stephanou, T., and R. Dagada, “The Impact of Information Security Awareness Training on Information Security Behavior: The Case of Further Research,” paper presented at the ISSA 2008 Conference, University of Johannesburg, 2–4 July 2008.