CLOUD BANKING IN AFRICA

THE REGULATORY OPPORTUNITY

HOW CLOUD BANKING CAN HELP REACH AND SERVE THE POOR

G:ENESIS UNLOCKING VALUE

orange™ Business Services

Document Reference: Cloud Banking in Africa: The Regulatory Opportunity

Date: October 2019

Contact Information

Genesis Analytics (Pty) Ltd - South Africa
Physical: Office 3, 50 Sixth Road Hyde Park, 2196, Johannesburg, South Africa
Postal Address: PO Box 413431, Craighall, 2024, Johannesburg, South Africa
Tel: +27 11 994 7000
Fax: +27 11 994 7099

Genesis Analytics Ltd - Kenya
Physical Address: 4th floor, West Park Suites, Ojijo Close, Parklands, Nairobi
Postal Address: P.O. Box 76608-00508, Nairobi, Kenya
Tel: +254 700 804 320

www.genesis-analytics.com

Orange Business Services – Dubai
Physical Address: Office 106, Dubai Islamic Bank Building, Dubai Internet City, Dubai
Tel: +971 4391 6900

www.orange-business.com

Authors

Genesis Analytics

Orange Business Services

Contact person

Richard Ketley
Email: richardk@genesis-analytics.com

Bavani Naidoo
Email: bavanin@genesis-analytics.com

Anastasia Smith
Email: anastasias@genesis-analytics.com

Pieter Zylstra
Email: pieter.zylstra@orange.com

ACKNOWLEDGEMENTS

We want to acknowledge the generous in-kind contributions from Serges Adingni (Islamic Bank of West Africa), Johnson Yapi (Bank of Africa), Damien Gueroult (BIMA Microinsurance), Joshua Ojo (African Development Bank), Steven Olowoyeye (Ecobank), Islam Zekry (CIB), Peter Kawumi (Interswitch Group) and Deusdedit Massuka (CRDB Bank).

We would like to thank and acknowledge the South African Reserve Bank, Central Bank of Egypt, Central Bank of Nigeria, Bank of Uganda and the Association of African Central Banks for their time and valuable insights on the regulatory landscape for cloud banking in Africa.

We would like to thank the Bill & Melinda Gates Foundation for supporting this project.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

INTRODUCTION

"Increasingly I manage a technology business"
Sim Tshabalala, CEO of Standard Bank.

Africa's development challenges remain formidable and poverty remains a critical issue in most countries. Addressing the challenges and improving livelihoods are linked to getting more Africans economically active. Access to financial services plays a key enabling role in supporting economic activity, protecting households from economic shocks and enabling savings and investment. Despite several decades of interventions to promote financial inclusion, the average rate of financial inclusion in Africa is just above 41% and there are approximately 717 million adults[1] in Africa who are financially unserved or underserved.

Part of the reason for this is the high cost of providing financial services, which forces many providers to remain focused on serving the wealthiest consumers, who can generate the required revenues to cover these costs. Many new technologies and ways of accessing technology allow for more agile, connected and cost-effective ways to deliver financial services - not just for mobile network operators (MNOs) who have pioneered the delivery of low-cost digital financial services, but for a much wider range of providers, including traditional banks. This report focuses on how cloud computing has the potential to unlock value for the providers and users of financial services through reducing costs and improving efficiency in a manner that promotes competition in the provision of financial services.

Cloud solutions allow financial service providers (FSPs) greater flexibility to deliver business applications through virtual shared infrastructure that reduces the cost of data storage and delivers capacity as it is needed. Commercial suppliers now provide a range of cloud strategies from both dedicated in-house infrastructure to global shared services from private clouds for proprietary use, to public clouds shared with other users and hybrid models that combine these for different business applications.

Internationally, cloud banking has become an important component of banking information and communication technology (ICT) strategies as it reduces the need for large upfront investments in ICT infrastructure. Instead banks pay vendors or cloud providers, using flexible models that charge for capacity when these are required and can adapt as market demands change. Outsourcing the ICT infrastructure also allows banks to better utilise ICT staff to focus on value-added activities, product development and innovation. The total ICT cost savings from cloud use can be substantial. Beyond cost savings, cloud services also allow banks to integrate data across business units and geographies, and with external third-party providers to deliver more innovative products to customers. Cloud banking thus reduces some of the barriers of entry to the financial sector and has the potential to change the scale economies of the sector, with the potential to reduce costs to consumers.

The providers of financial services are, however, not as free to optimise their technology infrastructure as they would like. Many of the decisions governing ICT infrastructure and its physical location are the subject of financial and national regulations. Well applied, such regulation ensures the safety and stability of the sector, protects the interests of consumers and ensures appropriate levels of business continuity and "system uptime". Poorly applied, the same regulations can burden the sector with legacy and uncompetitive cost structures that prevent the low-cost provision of financial services that are required for their widespread adoption – to the detriment of financial inclusion, economic development and poverty alleviation.

To date African regulators have remained cautious in their approach to regulating financial innovation in

[1] The Little Data Book on Financial Inclusion 2018, World Bank, 2018

which cloud banking plays an important part. Some regulators, such as the Kenyan Central Bank, have begun to facilitate fintech innovation through the use of innovation labs or sandboxes and the South African Reserve Bank has released a directive and guidance note detailing items banks must consider when electing to adopt cloud computing as a service – but most regulators have not taken a definitive stance[2]. This deters financial institutions from migrating to cloud technology and hinders the potential benefits to the financial services sector, preventing African consumers benefiting from the cost efficiencies and competition that would result from cloud banking.

This report will argue that regulatory frameworks across Africa need to be modernised to keep up with the evolution of technology, to ensure they do what they are intended for – promoting and protecting consumer interests by enabling FSPs to deliver the least cost, most efficient, safe and stable products and services. However, as much as cloud computing promises to improve the efficiency and competitiveness of the sector, many regulators have legitimate concerns on key issues. These issues include the oversight and management of data and the regulators' ability to protect data generated in their markets, the security of data that is stored virtually and is accessible over the internet, and the ability for FSPs to ensure service continuity in the face of mishaps on the cloud.

The report proposes a framework to assist regulators in navigating this modernisation journey. It explores how cloud banking can assist FSPs to provide low-cost digital services that are financially sustainable and competitive, and the role regulators need to play in re-visioning how they regulate financial service operations as businesses globally move to the cloud.

The first chapter of this report examines the financial services landscape in Africa and the challenges of providing cost-effective financial services to low-income consumers. It considers the number and relative size of FSPs on the continent and the challenges they face, the role of MNOs as a competitive force and the opportunities to develop a deeper and more competitive financial services sector. It examines how Africa's largest banks in its biggest economies are adapting to the digital world and also the opportunities technology presents for the hundreds of small banks and other FSPs in Africa. It also examines how MNOs have already tapped into the financial services market by providing low-cost transactional banking services to the previously underserved market through existing digital infrastructure.

The second chapter defines cloud banking by unpacking the different cloud services and deployment models, the benefits of adopting cloud technology, and the elements an FSP must consider when migrating to a cloud computing architecture. Among those elements are security and data protection, how to manage legacy systems, and the network and communication infrastructure required to make cloud technology feasible.

The third chapter is on the role regulators play to ensure the stability and security of the market as well as innovation facilitation methods used by regulators to encourage innovation while mitigating risks. It describes the stance other regulators have taken regarding cloud banking and the position of African regulators on cloud banking technology. The fourth chapter incorporates suggestions to enhance the regulatory framework of African markets to benefit from technology advances and cloud banking.

The final chapter concludes with a cost benefit analysis of cloud banking in Africa which weighs up the regulatory effort required with the benefits of cloud banking and how cloud banking creates more inclusive financial service sectors.

[2] In developing this report, key findings were shared with financial sector regulators in a wide number of Africa countries – including Nigeria, South Africa, Egypt, Uganda, Rwanda, Zambia, Tanzania, DRC, Tunisia, Guinea, Madagascar and BEAC. Their input and comments are very much appreciated, as is the support of the Association of African Central Bankers.

Part 1

A LARGE CONTINENT OF MANY SMALL BANKS AND LARGE TELECOMS

A LARGE CONTINENT OF MANY SMALL BANKS AND LARGE TELECOMS

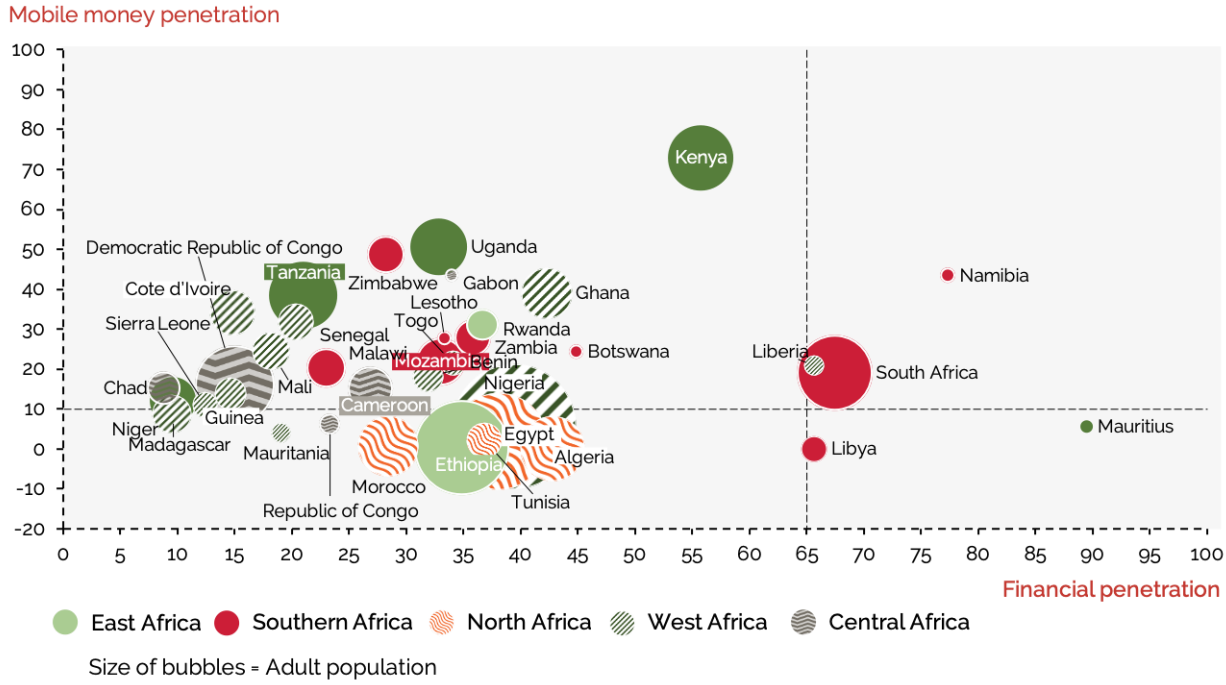
1.1. INTRODUCTION

This chapter explores the nature of financial service provision in Africa by analysing the structure and size of banks on the continent, and the role competitors play, both incumbent (MNOs) and emerging (fintechs). It considers the challenges faced by FSPs and concludes by considering the opportunity presented by technology and specifically cloud banking to improve access, reduce costs and improve the efficiency of financial services. It also considers the changing demographics and consumer behaviours on the continent, and the impact these will have on FSPs.

The rapid growth of mobile money on the African continent is a clear indicator of the demand for financial services from a large and mostly unbanked population. The rise of MNOs and their mobile money products began in response to the poor financial services infrastructure provided by banks in many markets, giving the underserved market access to a basic transaction account that can store, receive and send money, and has grown exponentially in markets with large rural populations and strong domestic remittance corridors where there is little access to banks or their branches.

While mobile money has made a significant impact on financial inclusion, the picture is far from complete. Figure 1.1 illustrates that most countries in Africa have financial inclusion below 45% while at the same time mobile money penetration remains below 50%. If it can provide products that are affordable and accessible, Africa's financial services sector should have considerable opportunity for growth.

Figure 1.1. Mobile money vs. banked population in Africa (2017)[3]



[3] *Source: Global Financial Inclusion Database, World Bank, 2017*

1.2 THE FINANCIAL SECTOR

The financial service provider landscape in Africa consists of a range of providers - from international banks, state-owned banks and co-operatives, to small local banks, microfinance providers and, increasingly, mobile network operators.

There are 774 banks that operate on the continent[4] that serve approximately 245 million consumers. When categorised by size[5], 90% of African banks are either tier three or tier four - defined by Gartner as a bank with an asset size of less than USD 5 billion. Only 6% of African banks are classified as tier-one banks with an asset size of greater than USD 10 billion. When compared with the largest international banks, their relative size becomes truly apparent.

Figure 1.2. African banks by tier[6] | % of total banks in each tier

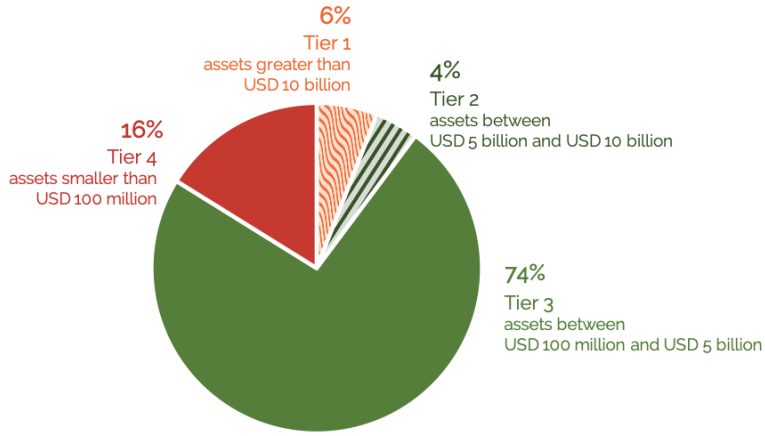
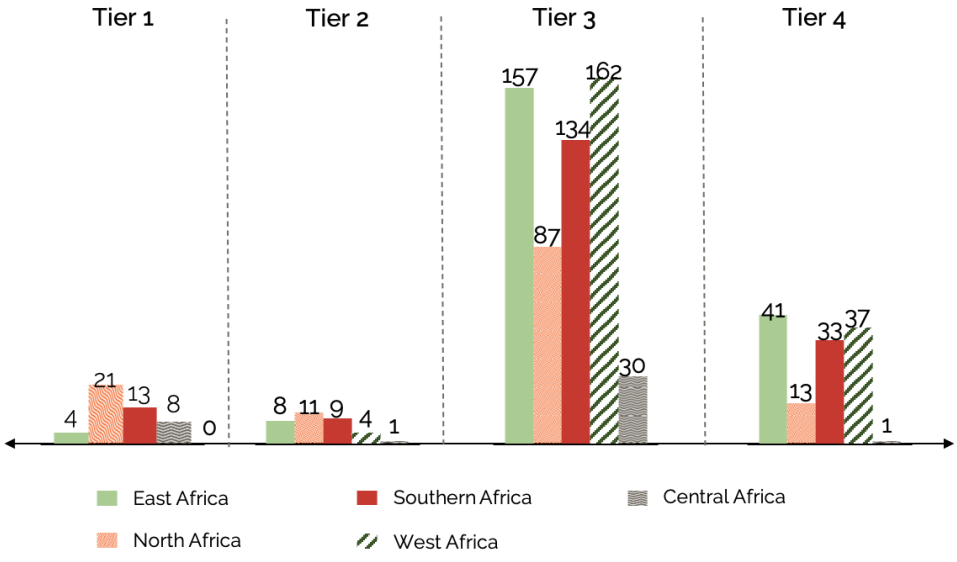


Figure 1.3. Distribution of African banks by tier and region[7] | Number of banks

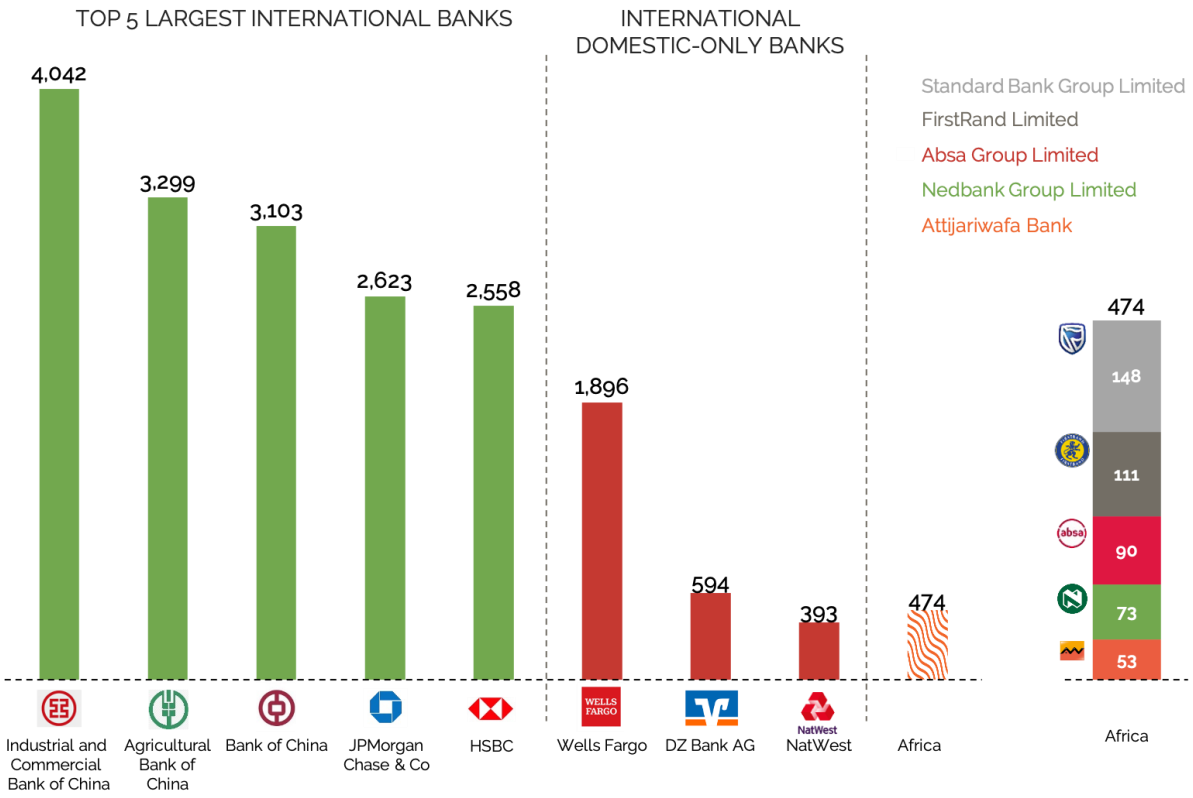


[4] Annual report data, Bank Focus, 2018
[5] Gartner Glossary: Bank Tiers, Gartner, 2018
[6] *Source: Bank Focus, 2018 | Gartner Glossary: Bank Tiers, Gartner, 2018*

[7] *Source: Bank Focus, 2018*

Standard Bank is Africa's largest bank with total assets of USD 148 billion, yet it ranks only 296th globally by asset size. The next largest African bank, FirstRand Limited, ranks 87 places down at number 383. The top five banks in Africa (of which four are in South Africa) have a combined asset size of USD 474 billion, just 20% of HSBC's total assets (the fifth largest global bank), or not much larger than an international, domestic-only bank such as NatWest in the UK with an asset size of USD 393 billion. Furthermore, small banks in Africa are tiny; tier-three banks have an average asset size of USD 974 million whilst tier-four banks have an average asset size of just USD 50 million.

Figure 1.4 Multinational banks, international banks and African banks by asset size (2018, USD billions)[8]



In addition to African banks being significantly smaller compared with their international peers, the majority of banking customers in Africa are served by the fragmented small-bank segment consisting of 695 tier-three and tier-four banks. About 65% of the banked population is served by tier-three and tier-four banks whereas only 35% is served by tier-one and tier-two banks. In contrast, six MNOs serve approximately 75% of all customers with active mobile money accounts across the continent.

[8] *Source: Bank Focus, 2018 | Bank annual reports, 2018*

Figure 1.5. Percentage of banked customers served by African banks by tier size[9]

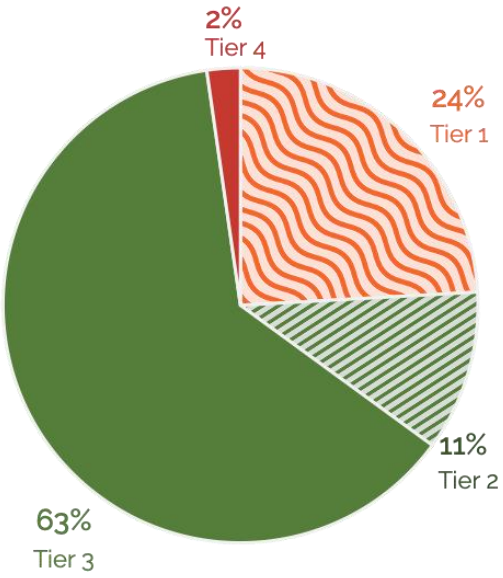
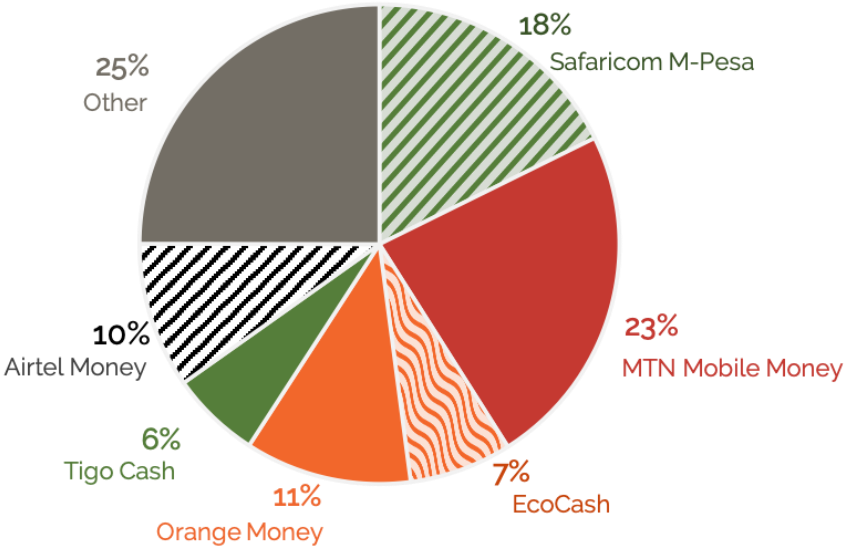


Figure 1.6. Percentage of customers with mobile money accounts served by MNOs[10]



[9] *Source: Genesis Analytics team analysis, 2019 | Global Findex Database, World Bank, 2017 | Roaring to life: Growth and innovation in African retail banking, McKinsey & Company, 2018 | Bank Focus, 2018 | Is Capitec now the biggest bank in South Africa, BusinessTech, 2018 | Banque du Caire, One of the Largest State-owned Banks in Egypt, Goes Live with Temenos to Redefine Digital Customer Experience, Bloomberg, 2019 | Citizenship Sustainability & Innovation Report, Union Bank of Nigeria, 2018 | Akiba Commercial Bank, Triodos Bank, 2015*

[10] *Source: MNO annual reports, 2018 | Global Findex Database, World Bank, 2017*

Table 1.1. A sample of Tier 1, 2, 3 and 4 African banks (2018)[9]

Region	Country	World Rank	Tier	Bank	Total assets (USD bn)	Cost income ratio (%)	Cost asset ratio (%)	Net income asset ratio (%)
Pan African	South Africa	296	1	Standard Bank	147.78	54.63	2.92	1.57
Southern Africa	South Africa	383	1	FirstRand	111.27	52.62	3.6	2.05
Pan African	South Africa	464	1	Absa Group	89.54	63.14	3.94	1.24
Southern Africa	South Africa	539	1	Nedbank Group	72.53	59.18	3.23	1.39
North Africa	Morocco	684	1	Attijariwafa Bank	53.31	48.13	2.19	1.37
North Africa	Egypt	2,212	2	Bank of Cairo	9.27	39.28	1.99	1.59
East Africa	Kenya	2,558	2	KCB Group	7.01	48.74	5.14	3.53
West Africa	Nigeria	2,692	2	Ecobank Nigeria	6.37	61.14	4.47	1.43
East Africa	Kenya	2,894	2	Equity Bank Group	5.63	49.22	5.69	3.61
West Africa	Nigeria	2,902	2	Fidelity Bank	5.6	70.52	4.62	1.48
Southern Africa	Angola	3,327	3	Banco Millennium	4.4	51.69	4.5	2.24
East Africa	Kenya	3,658	3	DTB Kenya	3.71	47.51	3.37	1.91
Southern Africa	Namibia	4,266	3	Bank Windhoek	2.76	52.94	3.62	2.22
West Africa	Ghana	4,714	3	GCB Bank Limited	2.22	59.84	7.57	3.21
Southern Africa	Zimbabwe	4,724	3	CBZ Bank Limited	2.21	58.24	3.98	3.00
East Africa	Tanzania	8,243	4	Amana Bank	0.1	93.12	8.61	0.29
East Africa	Kenya	11,148	4	Spire Bank	0.09	391.95	9.43	-22.14
East Africa	Uganda	11,384	4	Tropical Bank	0.08	95.73	11.87	-2.01
East Africa	South Sudan	11,579	4	Buffalo Commercial	0.07	36.78	10.90	13.09
Southern Africa	Mozambique	12,245	4	Capital Bank	0.04	123.72	14.31	-6.82

Africa's banking sector is also highly inefficient. Cost to income ratios measure efficiency by evaluating the operating costs against operating income. African banks have much higher cost to income ratios than their international peers, with the average cost to income ratio across all banks equating to 82.89%. The average cost to income ratio[11] across the top five African banks is 56% while the average across the top five international banks is 43%.

Despite their high costs, in terms of geographical coverage, Africa has the lowest branch coverage in the world, with just five branches per 100,000 adults[12]. Branches are still the most used channel on the continent, where 98% of respondents of a recent survey[13] said they use the branch to conduct banking business and more than two-thirds of Africa's customers admit to never having used POS terminals, internet banking, mobile banking or mobile payments. The branch model has contributed significantly to the high operating costs of banks.

Branches do not just serve customers. Many branches still have large back offices to support and execute transactions and processes such as account opening or credit assessments. Due to a continued reliance on manual and paper-intensive processes, there is a higher share of staff in support functions such as risk, marketing, HR and finance than international best practice[11].

Most banks on the continent still make use of and invest in "legacy" core banking systems deployed in the 1970s and 1980s[14]. These mainframe-based systems provide the foundational data housing and processing operations of the bank. Their design is often siloed – a business or product line's system operates independently from other systems. These legacy systems were not designed to be integrated or communicate with external systems. Data flows between these legacy systems require work-arounds and bolt-on solutions. According to Celent, a research and consulting company focused on financial services technology, ICT maintenance costs can be as high as 75% of bank and insurance company ICT budgets[15] due to the repeated application of these work-arounds, which increases the complexity of the legacy infrastructure.

This infrastructure has also constrained banks' ability to innovate. Fragmented sets of data repositories limit the extent to which banks can cross-sell products by using big data and data analytics solutions. Limited innovation is reflected in the low levels of digital transactions and banking sales, where only 16% of Africa's banking transactions and 4% of banking sales are digital compared with other international regions like Europe, where 82% of banking transactions and 19% of sales are digital, and Asia Pacific, where 82% of banking transactions and 17% of sales are digital[16].

Profitability in the sector has been maintained by pushing high costs back to consumers. Banking services in Africa are more expensive for consumers compared with other regions. The net interest margin spread in Africa is higher than in many other regions[17]. High interest spreads that often are the result of both high lending rates and low savings rates offered to customers have been a disincentive for consumers in taking up lending and savings products. Additionally, consumers in Africa often face high monthly account fees and high minimum balance requirements, which deter most African consumers who undertake small transactions and rely on subsistence incomes with little in the way of savings to maintain a balance on their account.

An analysis of a sample of African banks shows the average monthly fee for a standard transactional

[11] Annual report data, Bank Focus, 2018
[12] Roaring to life: Growth and innovation in African retail banking, McKinsey & Company, 2018
[13] Africa Banking Industry: Retail Customer Satisfaction, KPMG, 2016
[14] African Banking Survey, PWC, 2016
[15] Banks' ageing IT systems buckle under strain, Financial Times, 2015
[16] Roaring to life: Growth and innovation in African retail banking, McKinsey & Company, 2018
[17] World Bank, 2017

account is $4.67, which is significantly higher than the average from a sample of international banks' transaction account fees, which is $0.93[18].

Figure 1.7. Average interest rate spreads across regions (2015-2017, %)[19]

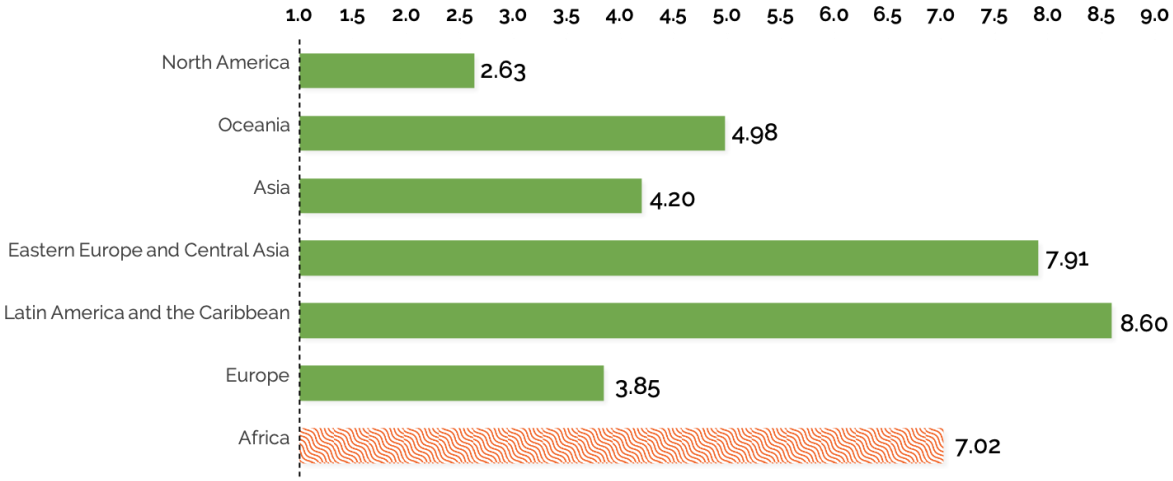
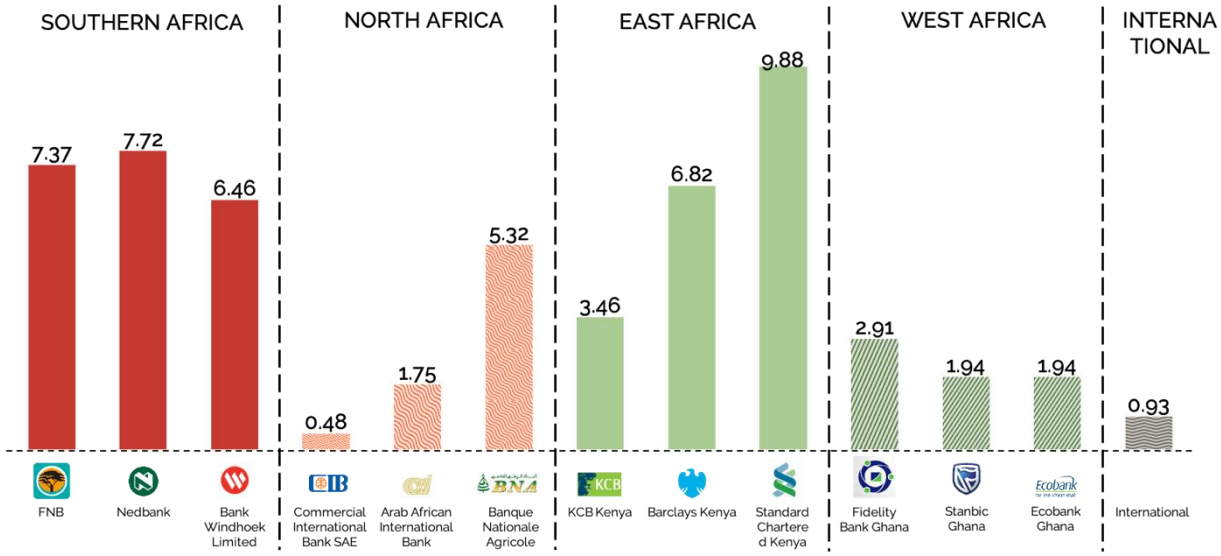


Figure 1.8. Comparison of current account monthly fees across regions (2019, USD) [20]



The traditional approach to banking products has excluded large portions of the population. Banks do not have a sense of who their customers are because customer data is inconsistent, often incorrect and

[18] Note many banks waive monthly fees if customer maintain a balance in their transactional account. These were included in the analysis as zero fee accounts.

[19] *Source: World Bank, 2017*

[20] *Source: Bank websites, 2019; South Africa's banking fees vs the world, Business Tech, 2018. Methodology was to find account fees for the standard cheque or transactional account and convert at the following exchange rates: 1 ZAR=0.07017 USD; 1 NAD=0.07017 USD; 1 EGP=0.05819 USD; 1 TND=0.33261 USD; 1 KES=0.00988 USD; 1GHS=0.19393 USD; 1 GBP=1.30167 USD; 1 AUD=0.70645 USD; 1 EUR=1.12197 USD*

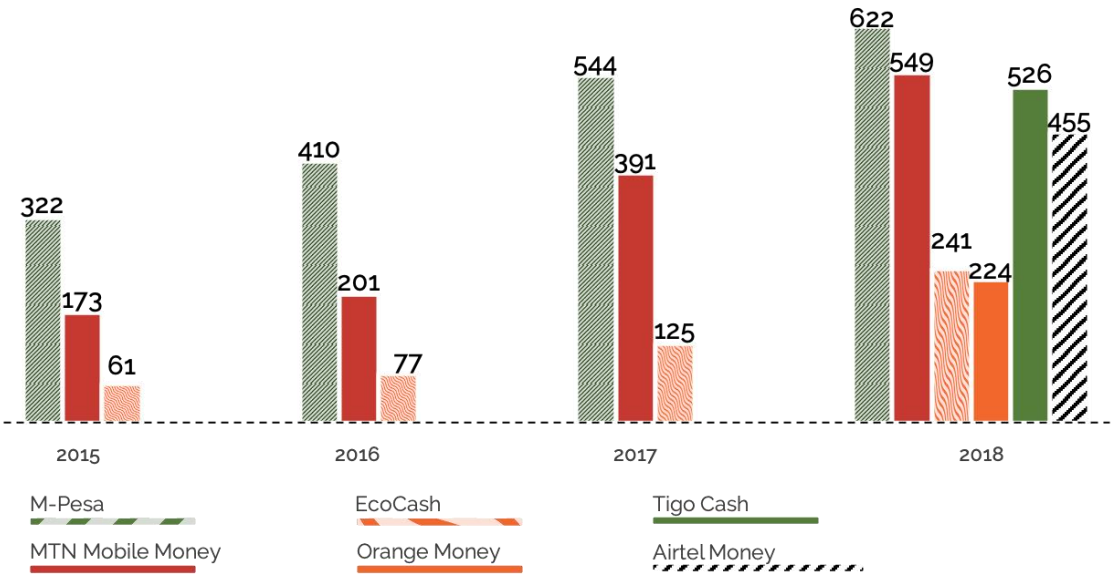
unintegrated, leaving banks with a limited view of what their customers' financial needs may be. In addition to this, banking products are relatively expensive for consumers, especially when most consumers complete only a few transactions a month. This has pushed consumers to look elsewhere for cheaper alternative financial solutions.

The difficulties and costs banks face in managing their technology infrastructure place them at a competitive disadvantage with respect to new entrants such as mobile money providers, who have the added advantage of operating under different regulatory regimes.

In many countries across Africa, MNOs have been much more successful in providing accessible and affordable products and services to consumers. MNOs have been able to provide mobile money services that leverage their wide agent network (originally established for pre-paid airtime sales), near universal mobile-phone penetration, and large customer base. Low know-your-customer requirements meant that it was easier to sign up customers and the frequency of airtime top-ups meant that customers were comfortable engaging with agents, and MNO brands enjoyed a significant level of trust. Across Sub-Saharan Africa such services accounted for 1.7 billion transactions, with a value of USD 26.8 billion in 2018, reaching over 395 million customers[21].

Some banks have attempted to replicate the success of the mobile money business model. Equity Bank in Kenya launched Equitel, a mobile virtual network operator (MVNO), in partnership with Airtel (an MNO). Equitel wallets are linked to bank accounts held at Equity Bank and customers are able to send money from their Equitel wallet to all other mobile wallets. The entity reached 22% market share in mobile commerce by value of transactions as at the end of March, 2018[22].

Figure 1.9. MNO mobile money revenues (USD million)[23]



[21] State of the Industry Report on Mobile Money, GSMA, 2018

[22] The Kenyan Wall Street; Equitel: Kenya's first and most successful MVNO; October, 2018

[23] *Source: Company annual reports, 2018*

Table 1.2. A sample of mobile money providers in Africa (2018)[24]

Region	Mobile Money Provider	Mobile Money Products	Total revenue from digital financial services (USD mn)	Value of payments (USD bn)	Volume of payments (mn)
East Africa	Safaricom	M-Pesa, M-Shwari, M-Tiba, Fuliza, M-Kesho	622	60	1700
South Africa	Econet Wireless	EcoCash, EcoCashSave	240.6	13	700 (since launch in 2011)
East & Central Africa	Airtel	Airtel Money	455.4	24	36

Mobile money service providers have expanded their product lines to include microcredit, which has become a major disruptor in markets such as Kenya and Tanzania. Safaricom's M-Shwari is a mobile banking service that is offered through the M-Pesa platform that allows consumers to make deposits into a mobile bank account, take out loans between USD 1 and USD 500 as well as open a savings account with no minimum savings requirement. MNOs are starting to look similar to banks as their product lines have become more sophisticated and focus on financial wellbeing, with products such as savings, insurance and wealth.

MNOs have been successful in broadening financial inclusion, but their business models are not without issues. Thus far it has been in the interests of MNOs to maintain closed platforms, and mobile-money account holders are limited to exchanging money with users of the same type of mobile-money wallet[25]. Limited operability is considered a factor in the fees that are charged for the services.

MNOs have been able to offer financial services by leveraging their investment in technology and distribution, originally established for the telecommunications business. They thus entered the market with a huge technological advantage at running systems that were built to handle many millions of micro-transactions. It is hardly surprising that in many ways they have eclipsed the role of many microfinance institutions (MFIs) that also targeted consumers and markets ignored by the banking sector.

Although the microfinance industry in Africa has been established for over 20 years, the industry's total gross loan portfolio is USD 10.51 billion and services just 7.02 million active borrowers[26], only 0.6% of Africa's total population. African MFIs face many challenges that have inhibited their capacity to contribute to the fight against poverty[27], including costly distribution and loan management models, and in contrast to MNOs, very limited use and ability to leverage technology.

MFIs in Africa also face a higher portfolio risk compared with other regions, which increases the cost burden and constrains the ability to expand financing.

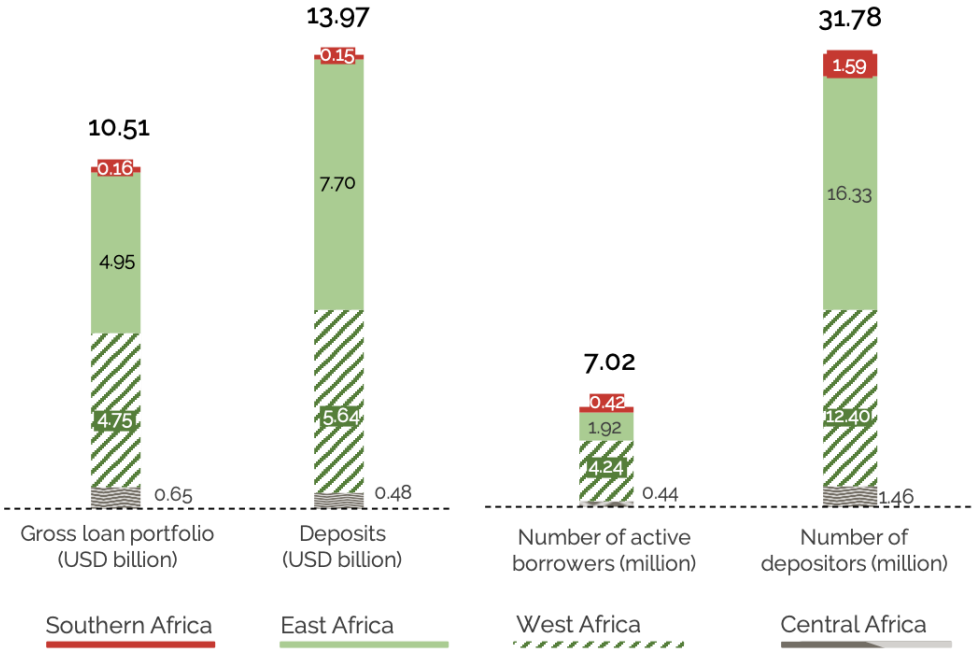
[24] *Source: Company annual reports, 2018 | M-PESA: how Kenya revolutionized mobile payments, N26 Magazine, 2018 | Sector Statistics Report, Communications Authority of Kenya, 2018 | Airtel to focus on mobile money as annual transactions pass USD 24 bn, The Exchange, 2018*

[25] Concept Note, Africa Fintech Summit, 2018

[26] Microfinance Information Exchange Market, 2018

[27] Microfinance in Africa, United Nations, 2013

Figure 1.10. Size of MFI industry by gross loan portfolio and deposits (USD billion), borrowers and depositors (million) (2018)[28]



Fintechs (finance startups leveraging technology to underpin their products or services) increasingly play a part in the value chain of financial services globally. With business models based on digital infrastructure that lowers their operational costs, as well as more flexibility and agility than large enterprises, they have been able to find innovative solutions to old challenges as well as develop completely new ideas.

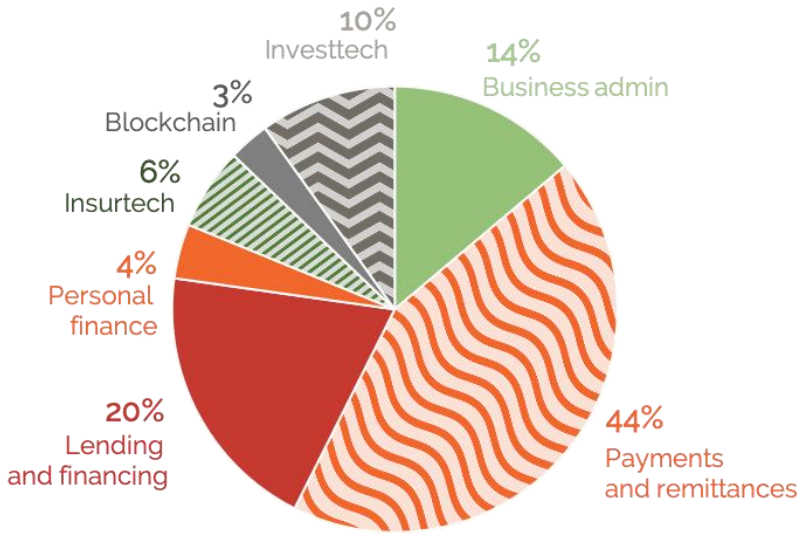
There are approximately 5,000 global fintechs, with over 300 startups active in Africa[29]. Fintechs in Africa are predominantly payments and remittances focused, where 132[30] fintechs focus on payments and remittances. Lending and financing follow a close second, which is aligned with the increasing need of consumers for lending and financing products. Most African fintechs are still in their infancy and as such have not been able to reach the full consumer population. As in many other markets, fintechs often require connection and the ability to integrate into larger platforms (be that an MNO, a bank, or a payment system). Across the world regulators are playing an active role in ensuring this outcome. The revised Payment Service Directive (PSD2), issued by the European Union, aims to contribute to a more integrated and efficient European payments market. Under the directive, banks will be required to provide third parties, such fintechs, merchants, and payment service providers, with access to their customers' accounts and customer data via application program interfaces (APIs). In Africa most fintechs have been left to fend for themselves, without enabling regulation. This serves neither their investors nor the interest of consumers.

[28] *Source: Microfinance Information Exchange Market, 2018*

[29] Fintechs in Sub-Saharan Africa: An overview of market developments and investment opportunities, EY, 2019

[30] Concept Note, Africa Fintech Summit, 2018

Figure 1.11. Types of fintechs in Africa (2018)[31]



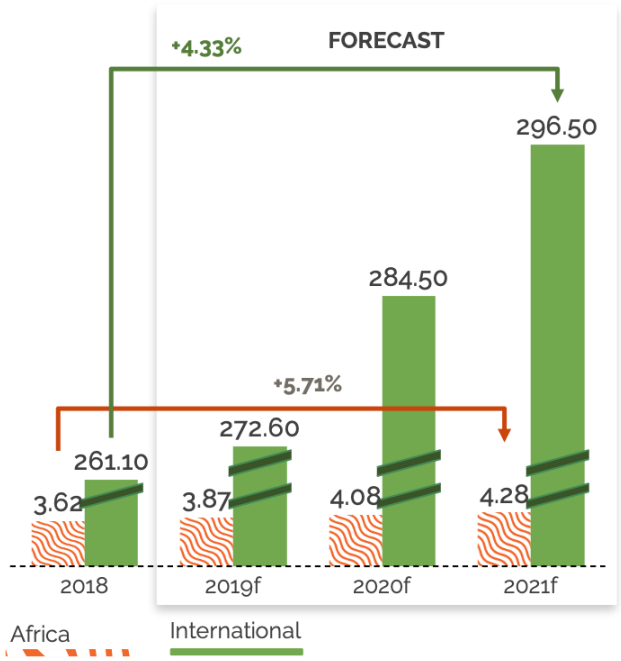
1.3 THE CURRENT COST OF THE ICT STACK

Many banks have acknowledged that to remain competitive in a digital world they need to become more efficient and lean in their operations. Banks are placing increasing emphasis on the importance of upgrading their technology infrastructure to integrate customer data across channels and create an enterprise-wide view of the customer. According to Ovum research (figure 1.12), global retail banking ICT spending amounted to USD 261 billion in 2018. Banks in Africa spent USD 3.6 billion in 2018 and this spending is estimated to increase at a CAGR of 5.71% until 2021. South Africa's big four banks, namely Nedbank, Absa, Standard Bank and FNB, alone spent over USD 2.15 billion on their ICT operations[32], suggesting the actual spend across the continent is underestimated.

Much of the spending is on software updates that need to be up to date to protect bank data[33]. Collectively the ratio of ICT costs (as the sum of amortisation and depreciation) to assets in South African banks is almost double that of the top four banks in the United Kingdom[34].

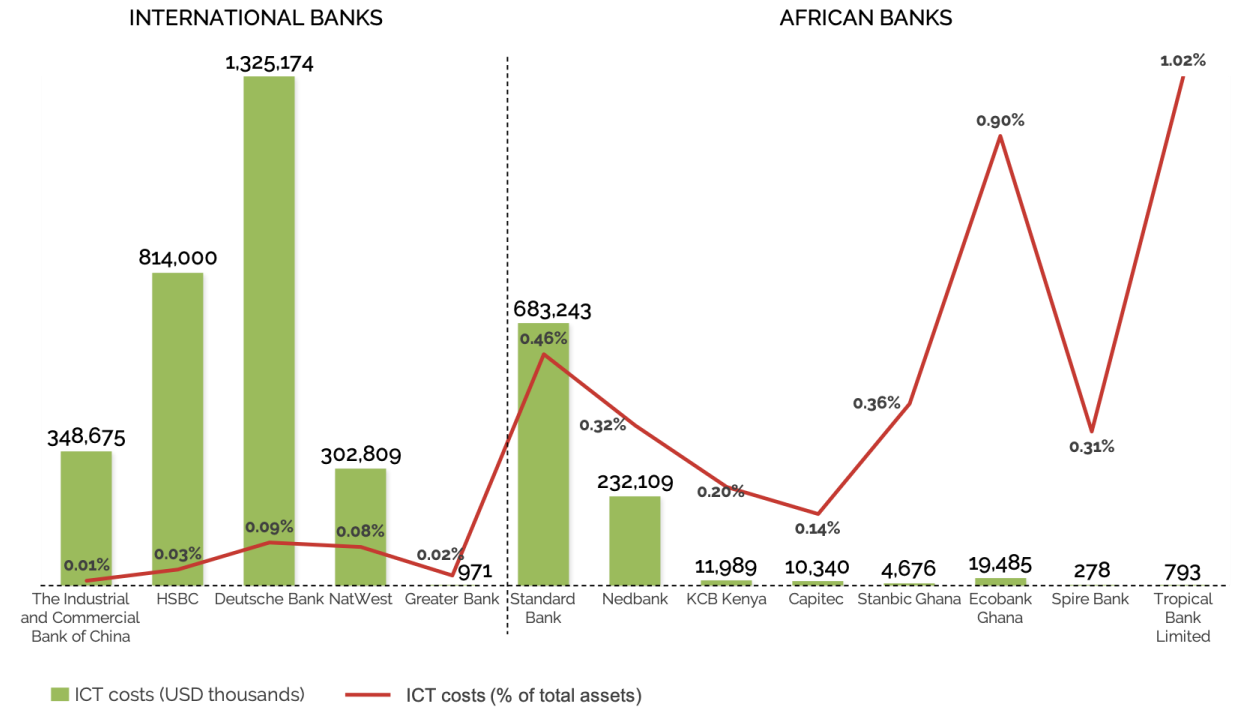
[31] *Source: Concept Note, Africa Fintech Summit, 2018*
[32] How much SA's big banks spend on IT, H. Tarrant, 2016
[33] Seven banks make N8.58bn fresh investments in software, I. Ogunfuwa, 2018
[34] Calculations using bank annual reports, Genesis Analytics, 2017

Figure 1.12. International and African Retail Banking technology spending (2018-2021, USD billion)[35]



Compared with international banks, the nominal amounts spent by African banks on technology seem small. However, when the small asset size of African banks is considered, the relative cost of technology is significantly higher. Figure 1.13 shows the average ICT cost to assets ratio across a sample of international banks is approximately 0.04% whereas the average ICT cost to assets ratio across a sample of African banks at 0.46%. The enormous cost of managing and integrating legacy systems is prohibitive and limits banks' ability to innovate to meet customer needs, or to reduce costs.

Figure 1.13. Relative cost of ICT at banks (2018)[36]



[35] *Source: Report on African Retail Banking Technology Spending, Ovum, 2018 | Global Tech Spending Forecast: Banking Edition, Celent, 2018*

[36] *Source: Annual report data, Bank Focus, 2018*

1.4 THE NEED FOR CHANGE

Although African banks have been falling behind on productivity, thus far they have been able to pass this on to consumers by way of higher margins and fees. But competitor models from MNOs, fintechs and new digital banks that use digital infrastructures are offering customers cheaper and more efficient alternatives, which limit the scope for such pricing strategies. The high costs and inefficiencies of traditional African banks will make it difficult for them to compete against digital banks and MNOs. In order to keep up with MNOs and fintechs, banks will need to evolve to have low-cost operating models that are acceptable to their regulators, who will need to encourage the use of innovative technologies. In the next chapter we unpack the concept of cloud banking and why it is such an important development in addressing the cost of technology for the complete range of FSPs that operate on the continent. We also explore the different service and deployment models available and the broader considerations (such as security, migration strategies and network requirements) to assess feasibility.

Part 2

CLOUD BANKING

CLOUD BANKING

2.1 INTRODUCTION

Cloud banking is about the use of cloud computing by FSPs. Cloud computing involves using internet technologies to provide virtual ICT infrastructure that is scalable and delivered as a service[37]. Historically, FSPs have had to invest in hardware and software assets that require large amounts of capital that are then depreciated over time. Cloud computing can change how FSPs consume technology by moving away from a model of consuming ICT products to one of consuming ICT services, where the hardware or software is rented on a needs basis.

The move to cloud banking often involves more evolution than revolution - the pace of which is determined by the enabling (connectivity and cost) and the regulatory environment. The widespread use of the internet and improving connectivity have allowed many FSPs to use cloud-based services for non-core and non-critical uses, such as human resources and email, customer relationship management and some document storage. However, the transition to cloud core banking services (such as treasury, transactions, product and account management, payments, etc.) has been slower due to the particular nature of the risks and regulations in banking. This chapter outlines some of the core concepts and issues in the adoption of cloud banking.

2.2 CLOUD SERVICE AND DEPLOYMENT MODELS

Cloud computing can involve three main service models - Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).

The SaaS model offers users access to application software from a device with an internet connection and web browser[36]. SaaS provides users with a completed product that is run and managed by the provider; users have control of only the configuration settings specific to the application. Applications are either free or paid through a subscription and their accessibility facilitates collaborative working. In most cases, SaaS refers to end-user applications such as web-based email products – gmail being the most famous and ubiquitous. However, other SaaS services are widely used by banks, including platforms such as Salesforce for customer relationship management. Many African banks use the SaaS model for non-critical office productivity applications, such as Microsoft Office applications.

The IaaS model allows users to access computer infrastructure resources, such as processing power, storage, servers, networks and other resources, and enables businesses to run their own operating system and applications on this virtual infrastructure[36]. The virtualisation of infrastructure allows many users to share one physical server. Of all the service models, IaaS has the highest level of management and control by the bank's ICT department because users are able to control storage levels, the operating system and specific network components.

The PaaS model offers a computing platform from which users can run and develop their own applications, using libraries, languages, databases, tools and other providers' resources[36]. In other words, it is a platform for creating software that is delivered online. This service model entails a higher level of management and control by the cloud provider compared with IaaS where users can control only their own applications that run on the platform as well as the platform's configuration settings.

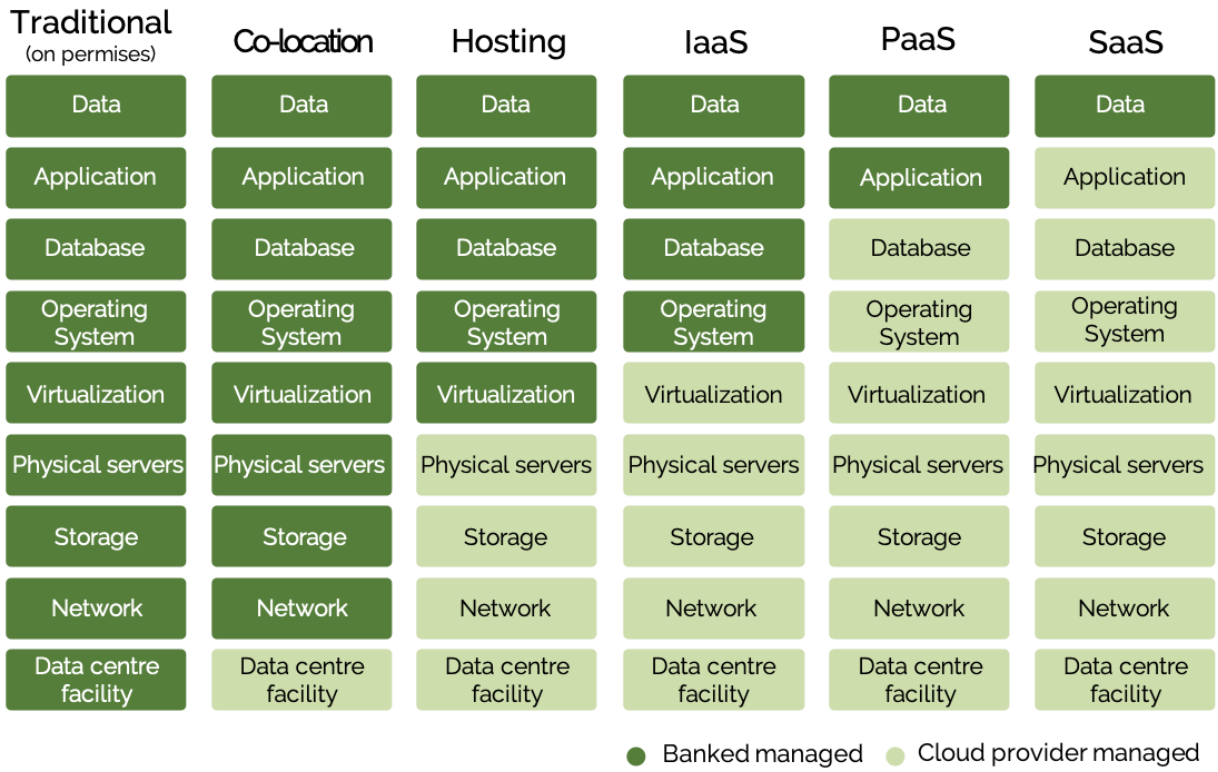
[37] Gartner IT Glossary: Cloud computing, Gartner, 2019

In a cloud deployment, FSPs do not manage or control the underlying ICT infrastructure (networks, storage, data centres or servers) as shown in Figure 2.1.

IaaS is more appropriate for applications that are resource intensive and where FSPs want to have control over the application, data and operating system. PaaS is more appropriate for applications that are in the development stage or undergoing testing. SaaS is more relevant for applications where the FSP does not want to control applications, due to a lack of skills, as well as applications that are not resource intensive.

Figure 2.1. Level of management and control of cloud services[38]

The evolution of cloud computing is already moving to multi-dimensional service models that focus on both



technical and business aspects, such as Business Process as a Service (BPaaS), Cloud Management as a Service (CMaaS) and Blockchain as a Service (BaaS)[39].

BPaaS is the delivery of business-processing outsourcing services, such as payroll, printing, ecommerce, which are all sourced from the cloud[55]. This service model aims to bridge the gap from business process to cloud computing by offering a distributed, multi-tenant capable workflow engine where users can upload customer executable business processes and access external services[40].

CMaaS provides the management of the different cloud environments. Users are able to manage the deployment and operation of applications and associated datasets across multiple cloud service infrastructures[41]. Cloud management services are essential in enabling visibility, simplifying management and optimising the utilisation of resources in a multi-cloud environment.

Beyond a decision around the services an FSP wishes to procure from a cloud provider, there is also a

[38] *Source: Cloud Banking or Banking in the Clouds, BBVA, 2016*
[39] Gartner IT Glossary, Gartner, 2019
[40] A Cloud-driven view on Business Process as a Service, J. Domaschka et al., 2017
[41] Practical guide to cloud management platforms, Cloud Standards Customer Council, 2017

decision around the type of deployment model. The main difference between the deployment models relates to where the infrastructure resides and who has control of the infrastructure[42].

Public cloud is openly available for use by multiple users. Users pay for the services of a public cloud on a pay-as-you-use basis. Public cloud has unlimited scalability, where computing resources are available according to demand. The public cloud model is a reliable deployment model because business continuity is supported by a large network of servers. It is fast to implement and integrate this model within the organisation, which reduces the time-to-market[41]. However, due to multiple users the public cloud is more susceptible to cybercrime as data is highly concentrated.

On the other end of the spectrum, a private cloud model is available for the exclusive use of a single organisation where there is increased flexibility relative to the public cloud as computing resources can be customised according to the organisation's requirements. The organisation has more control of the cloud and a higher level of security because resources are not shared with any other organisation. Additionally, private cloud ensures that there is data preservation during a system outage. In this model, the infrastructure can be either hosted on site, as an internal cloud that is in-house, or off site where the cloud service provider (CSP) owns and operates the cloud[41]. Private clouds are more expensive than public clouds because they require more investment, but are better suited to businesses with concerns around data security and privacy.

The hybrid cloud model is the composition of two or more distinct deployment models that retain unique infrastructures but are interconnected to allow for data portability. This deployment model is cost effective because user organisations pay for the computing resources only when they need them. The model offers maximum flexibility as additional resources of the public cloud can be made available whilst still maintaining the security of a private cloud model for sensitive data. Like the private cloud model, the hybrid model provides data preservation during a system outage[41]. However, this model is the most complex option in terms of deployment and management. Furthermore, the probability of vendor lock-in is higher for the hybrid cloud model compared with public, community and private clouds as migration is more complex, and hence banks will be more reliant on the CSP.

FSPs of all sizes in Africa are beginning to explore cloud deployment strategies often on the hybrid cloud model, where they combine the cost savings of public cloud infrastructure with the enhanced security of the private cloud model[43]. Public cloud deployments are used to host non-critical office productivity tools used by employees (such as email), as applications used by employees are subjected to less strict/unclear cloud regulation. Enterprise resource planning (ERP) applications (such as HR, finance and procurement) are being migrated to private clouds[42].

The community cloud model is available for the exclusive use of a specific community of users or organisations that have shared interests. This model is cost effective because organisations can share the costs of a private cloud model for specific community needs. However, the total cost will most likely be higher than the public cloud. Similar to the public cloud model, the community cloud model is highly scalable where computing resources are available according to demand. The level of security is higher than that of the public cloud model and it can be tailored according to the community needs[44].

For banking applications that require extra security, i.e. applications that deal with confidential customer financial data, a private cloud is the most appropriate model for a large bank. Private cloud will provide financial institutions with the highest level of security as data centres reside within the firewall. Since the

[42] FSI Insights on policy implementation No 13 - Regulating and supervising the clouds: emerging prudential approaches for insurance companies, Bank for International Settlements, 2018

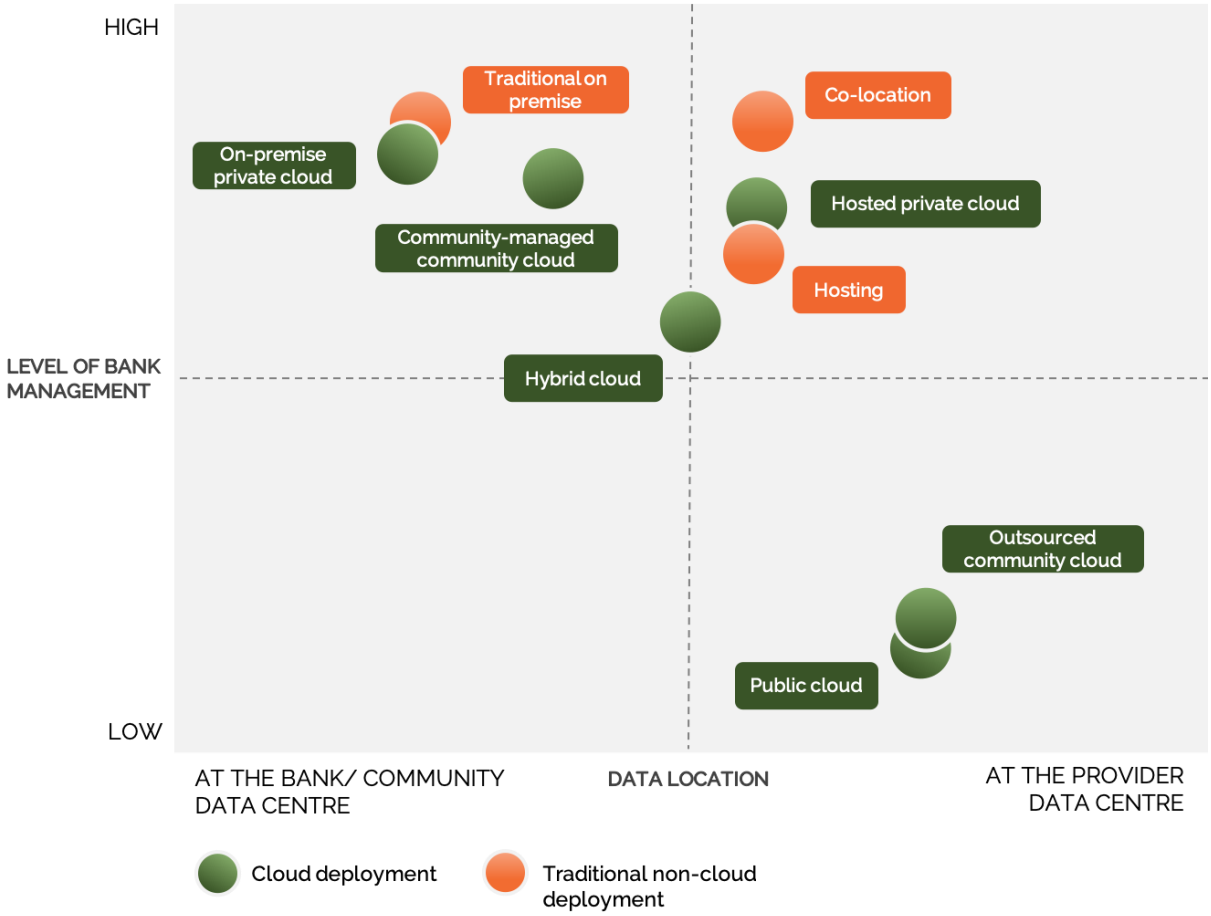
[43] Interviews with select African banks, Orange Business Services, 2019

[44] FSI Insights on policy implementation No 13 - Regulating and supervising the clouds: emerging prudential approaches for insurance companies, Bank for International Settlements, 2018

financial institution owns the cloud platform, there is a high control over confidential information. The hybrid and community cloud models could be an option for smaller regional banks because there are the benefits of cost savings. Extra scalability, however, requires extra deployment efforts.

For applications that are less critical and do not contain customer financial data, the public cloud would be the most appropriate model. Microsoft Office applications and internal web applications are good candidates to be stored on the public cloud because these types of applications are usually used only during working hours and the bank would only pay for these applications on a pay-as-you-use basis. Furthermore, these types of applications scale faster than other applications.

Figure 2.2. Level of bank management and location of data for different cloud models



2.3 LEGACY ICT INFRASTRUCTURE

One of the biggest challenges banks in particular face is managing and changing their current infrastructure. The current infrastructure of banks can be likened to a jigsaw of siloed legacy systems (developed in the 1970s) and newer external systems.

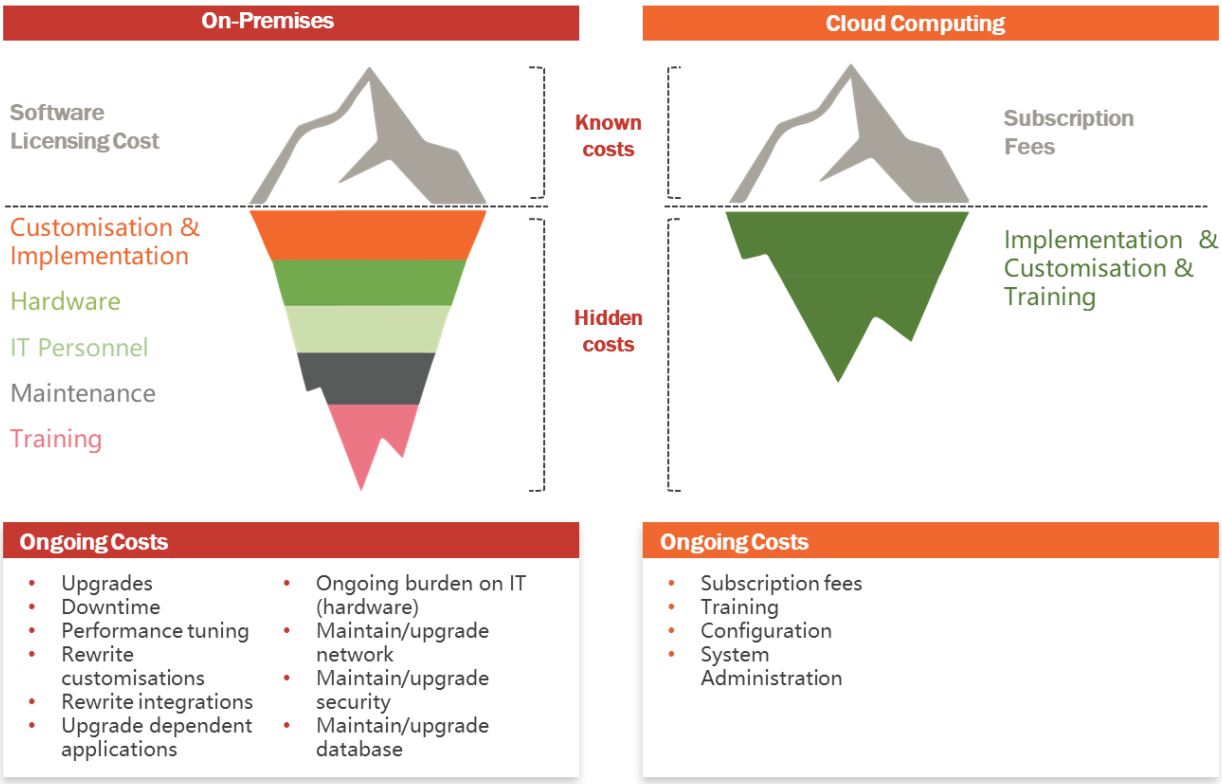
Due to the complex nature of legacy ICT systems, it has become more and more costly to integrate new channels and offerings that often need to be integrated into an array of applications and databases. For instance, integrating a new channel (such as a banking app) into traditional bank ICT structure would potentially require integration into dozens of systems and platforms. Banks have attempted to build integration layers between traditional ICT systems to decouple specific applications from dedicated databases and unlock data, as well as integrate and analyse the data across various digital channels. The integration of systems and banking applications continues to be a major cost and challenge for banks' ICT departments. The integration and sharing of data through application programming interfaces (both internally and externally) are now at the heart of banking innovation, and in solving these challenges. Application programming interfaces (APIs) are the software used to build applications that facilitate the interchange of information between platforms.

The modulisation of this architecture and integrations that can be managed in the cloud by specialist vendors using standard interfaces have the potential to dramatically reduce the complexity and cost of managing a bank's infrastructure. This is even more so when the core infrastructure also resides in the cloud. The modular architecture enables the introduction, removal and upgrading of modules (products, services, processes, etc.) without jeopardising the integrity of the system. At the heart of modular architecture is cloud computing, where banks are able to renew systems faster. It also enables the banking-as-a-platform business model where the platform owner (the bank) maintains management of the customer experience while adding third-party products and services that will enhance the customer experience.

2.4 CASE FOR CLOUD BANKING

Cloud banking provides the opportunity for banks to significantly lower their ICT costs. There is increased flexibility in terms of paying for only what you need and use and none of the costs around having to upgrade to the latest technology. Cloud banking allows banks to book resources (processing capacity, software, storage capacity etc.) dynamically on demand and release excess resources when they are no longer needed. This results in the bank paying less for ICT infrastructure and services and achieving higher utilisation on ICT spend. The cost of running a specialised ICT department also falls and banks no longer have to invest in ICT skills. For small banks in small markets where such staff may be in short supply, cloud computing can ease a critical operational constraint. Fixed costs are also converted to a subscription-based approach and upfront capital investments are converted into operational costs.

Figure 2.3. On-premise versus cloud banking costs[45]



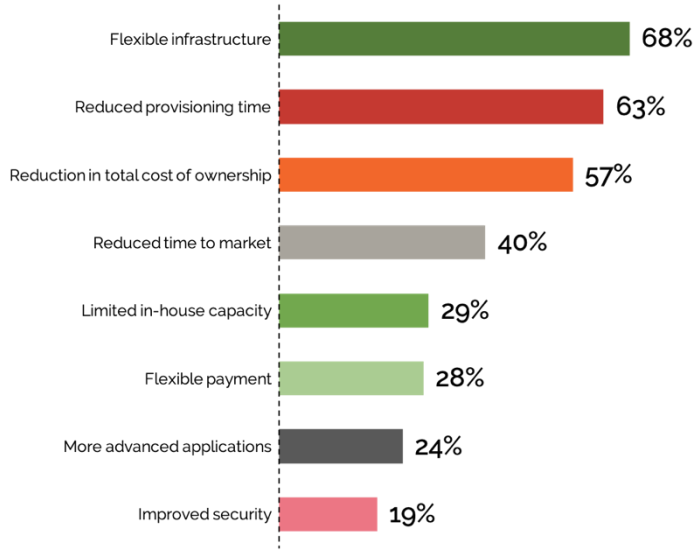
The most compelling reason to move to cloud is undoubtedly cost savings, but there are other business reasons too. The flexibility of cloud-based operating models allows banks to experience shorter development cycles for new products because teams do not need to first make capital investments for new infrastructure, decreasing the set-up time required. This supports a faster and more efficient response to the needs of banking customers.

Cloud servers improve the accessibility of third parties to bank data and operations by removing the need for these parties to be on site. Subsequently banks may collaborate with foreign firms to make use of sophisticated analytics capabilities that are unavailable, or more expensive to access locally. Analytic models run on the vast amounts of customer data held by a bank. Data mining capabilities examine such data to provide customer insights that help banks understand customer behaviours (e.g. where or when customers are most likely to visit a branch). Banks can then plan around these insights. Cloud technology provides the computing power necessary to deliver these insights in real time.

Additionally, cloud banking could improve business continuity for banks, where the cloud provider is responsible for ensuring that the technology is operational. The CSP is fully responsible for the risk mitigation of the banks' operational systems that are in the cloud. Banks can gain a higher level of data security, resilience, fault tolerance and disaster recovery from cloud computing. Cloud computing also provides a high level of redundancy and backup at a lower price than traditional managed solutions.

[45] *Source: Be aware of hidden costs of an on-premise core banking system, Oradian, 2019*

Figure 2.4. Select primary reasons for adopting cloud computing[46]



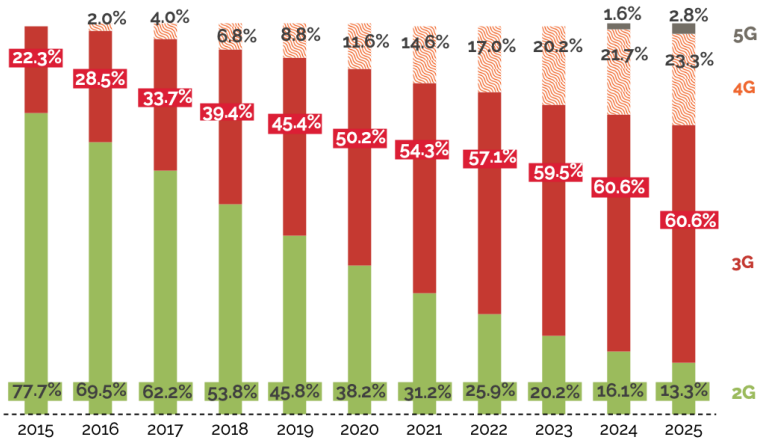
Cloud technology is helping banks move from product-centric business models to a customer-centric model, as banks' channels and products, and therefore customer data, are integrated, allowing for deeper customer insights. To the extent that cloud banking reduces the technology costs of any FSP, in competitive markets this should translate to a declining cost to serve, allowing FSPs to reach new and lower-income customers.

2.5 NETWORK CONSIDERATIONS

An important consideration for FSPs will be to assess whether there is sufficient and adequate market infrastructure available to support cloud computing. The greatest barrier to adoption and effective utilisation of cloud computing centres is the availability of a good internet connection[47]. Cloud banking requires extensive and affordable broadband access.

Despite major advances in mobile connectivity and internet access, many African countries continue to lag behind other regions of the world in mobile connectivity. The majority of cellular networks in Africa are 2G in rural areas and 3G or 4G in urban areas, compared with developed markets where 5G connectivity is becoming available. Applications involving the Internet of Things, big data, artificial intelligence (AI) and cloud computing typically require 4G or even 5G networks.

Figure 2.5. Evolution of mobile networks in Sub-Saharan Africa[48]

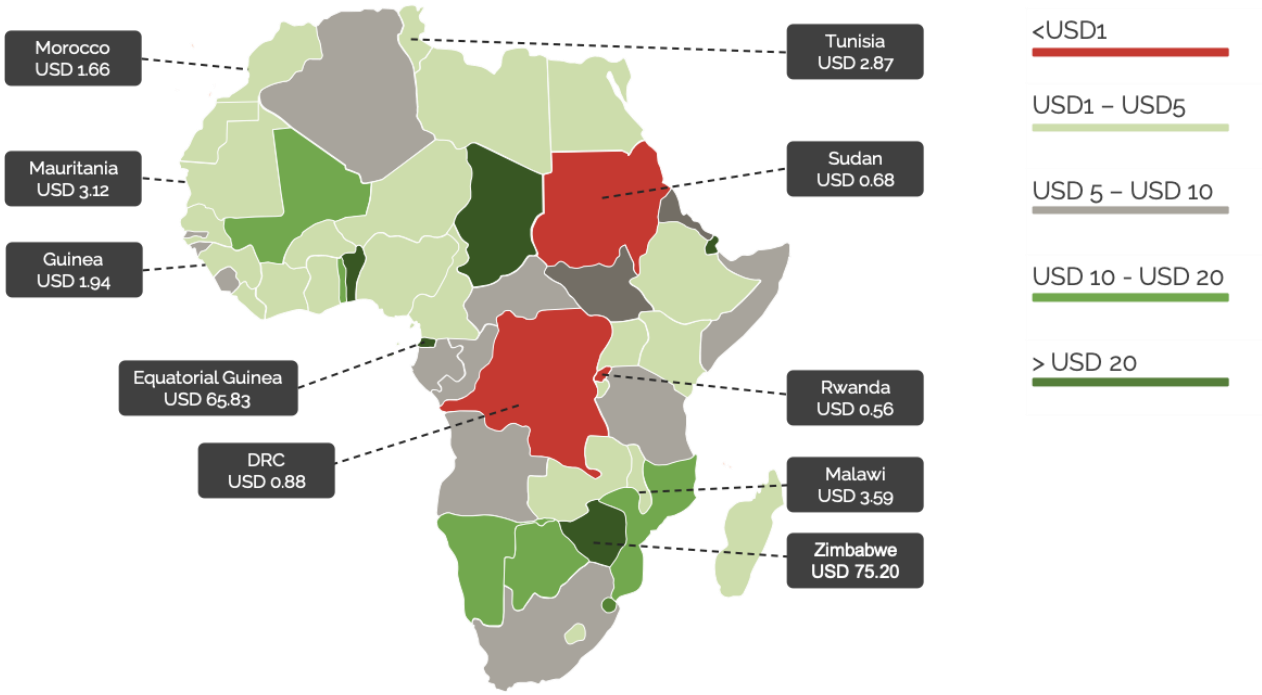


Equally important to the adoption of cloud computing is the cost of data. A 2018 study[49] analysed data plans across 230 countries to compare the cost of one gigabyte (1GB) of mobile data. While the most expensive country to buy data in is in Africa (where the average price for 1GB of data in Zimbabwe is USD 75.20) encouragingly it also found that 10 out of the top 50 cheapest countries in the world for mobile data are in Sub-Saharan Africa (Figure 2.6). Rwanda

[46] *Source: How cloud is being used in the financial sector: survey report, CSA, 2015*
[47] Cloud computing: Adoption issues for Sub-Saharan African SMEs, A. Dahiru et al., 2014
[48] *Source: GSMA Intelligence, 2018*
[49] Cable.co.uk

and Sudan feature in the top 10, with 1GB of data costing just USD 0.56 and USD 0.68 respectively[50].

Figure 2.6. Average price of 1GB of data (USD) [51]



One way of assessing the readiness of markets in Africa for cloud computing is to consider the ICT Development Index (IDI), which measures and monitors developments in ICT between countries annually. The IDI aims to measure the level and evolution over time of ICT developments within countries and the experience of those countries relative to others. It examines the progress in ICT development in both developed and developing countries, the digital divide and differences between countries in terms of their levels of development, and the development potential of ICTs and the extent to which countries can make use of them to enhance growth and development in the context of available capabilities and skills[52]. The IDI is divided into three sub-indices, namely: access, use and skills sub-indices. The final IDI score for a country is rated out of 10.

Africa has the lowest regional average for the ICT Development Index score at 2.64 compared with Europe, which has the highest average of 7.5, followed by the Americas at 5.21. The world average score for the IDI is 5.11. The average fixed broadband penetration in Africa is below 1% and is the lowest in the world, compared with the developing country average of 7.4% and world average of 11.2%.

Until 2010, Sub-Saharan Africa had been the most underserved region in the world in terms of international fibre capacity, particularly in East Africa, which relied exclusively on costly and less reliable satellite connections. Due to increased support for telecom infrastructure projects, including the focus by submarine-cable suppliers on potential market opportunities in Africa, international internet bandwidth is starting to improve in several countries[53].

The East African Cable System (EASSy) consists of a 10,000km fibre-optic submarine cable along the

[50] Worldwide mobile data pricing: The cost of 1GB of mobile data in 230 countries, Cable, 2018
[51] Worldwide mobile data pricing: The cost of 1GB of mobile data in 230 countries, Cable, 2018
[52] The ICT Development Index: conceptual framework and methodology, International Telecommunications Union, 2017
[53] Towards improved access to broadband in Africa, United Nations Economic Commission for Africa, 2017

East African coast, linking Sudan to South Africa with landing points in these countries as well as in Djibouti, Somalia, Kenya, Tanzania, Madagascar, Mozambique, Mayotte and Comoros. EASSy has provided the opportunity for access to cheaper high-speed international bandwidth across in the region.

The West Africa Cable System (WACS) consists of high capacity fibre-optic submarine cables that provide linkages between the countries in West Africa and Europe. WACS provides high-speed connection with low latency over its 14,500km route and has 12 landing points in Africa, namely South Africa, Namibia, Angola, Democratic Republic of Congo, Republic of Congo, Cameroon, Nigeria, Togo, Ghana, Côte d'Ivoire and Cape Verde. The landings in Namibia, the Democratic Republic of Congo, Republic of Congo and Togo provide the first direct connections for these countries to global submarine-cable network.

Some of the landlocked SADC countries are still struggling with slow and unreliable broadband access despite the deployment of undersea fibre cables[54].

The underdevelopment of fixed connectivity in Africa thus continues to constitute a challenge and obstacle to fully benefiting from advanced ICTs[55] in some countries.

In order to achieve an adequate level of IT infrastructure to support cloud-computing access, African regulators will need to provide the appropriate spectrum and implement policies and regulations that incentivise investment in broadband infrastructure and laws that ensure there is universal access to broadband networks.

2.6 SECURITY RISKS/CONSIDERATIONS

There has been much debate around the security of cloud models, due to the sensitive nature of data stored by banks. One of the major barriers to cloud adoption for African banks are concerns over security and compliance[56]. When implementing cloud services, banks give up control to the cloud provider regarding cloud infrastructure and other issues that may affect security. This is a significant loss of governance/control, which could adversely affect the reputation of the bank. Banks could also face the risk of being locked in by one cloud provider if they strongly rely on the services, which will make it difficult to migrate to another provider or back to an in-house ICT environment[57]. CSPs usually store and process data in different locations and sometimes between different clouds. This makes it difficult for banks to monitor whether cloud providers are compliant with data protection legislation[56].

The choice of deployment model and network connectivity will always result in trade-offs between security, accessibility and performance. For instance, a dedicated WAN link to the cloud will allow banks more control over performance and security but it will mean that the applications and workloads can be accessed through the internet, introducing risk.

Within the cloud environment there could be several technical failures that will impact cloud users. One of the technical risks is an isolation failure where failures or attacks in shared environments may cause a tenant to have access to another tenant's data.

Cloud environments are vulnerable to external attacks through the internet, as the APIs that are used to manage and interact with the cloud services are connected via the internet. Attacks on the cloud could not just be from external actors but also from within the cloud provider, where an insider could abuse their role

[54] SADC not bridging the digital divide, AfricaPortal, 2018

[55] Measuring the Information Society Report 2017, International Telecommunications Union, 2017

[56] Interviews with select African banks, Orange Business Services, 2019

[57] FSI Insights on policy implementation No 13 - Regulating and supervising the clouds: emerging prudential approaches for insurance companies, Bank for International Settlements, 2018

to access client data. When using cloud infrastructure, banks also have reduced visibility of the physical location of data and this makes it difficult to verify complete data deletion. This increases the risk that not all the information will be deleted from all the cloud providers' resources.

Despite the security risks that cloud users could face, there are some security gains that users could benefit from, especially small banks which are unable to invest heavily in the procurement of security technology and have limited expertise around security. In a future where cybersecurity is the main concern, large cloud providers (such as Microsoft, IBM, Amazon, Google, Alibaba and Liquid Telecoms) are capable of making the massive investments required to develop built-in security in their cloud platforms and regularly update the security to keep systems as secure as possible. Cloud computing provides platform uniformity, which makes it simpler and faster to provide platform hardening and automation of security operational tasks such as security patching, vulnerability testing and security audits.

On-premise data facilities are vulnerable to security risks and will require greater investment to maintain adequate levels of security. Cloud providers are able to hire a dedicated team entirely focused on security issues. This team is able to act faster to security breaches than a team that is assigned to multiple tasks in a banking environment. The security expertise and technology of CSPs are safeguards that small banks can easily leverage off to improve their operations. Public cloud environments could significantly benefit the majority of small and tiny banks in Africa, where the cost of routinely upgrading security software would be unaffordable.

2.7 MIGRATING TO CLOUD

Depending on the migration approach to cloud, FSPs could face high costs of migration. There are several factors that influence the cost of migration to the cloud: skills and knowledge of IT staff, application complexity, and compatibility of local servers.

Implementing cloud requires significant learning efforts of cloud services and tools because the cloud environment rapidly evolves. If an FSP's IT staff are knowledgeable on cloud and have the sufficient skills, then the training process is quicker and less effort is required. Migration costs will be higher if the application's complexity is high because it requires more effort to study and modify the application. If the cloud platform and local servers are similar, there will be less compatibility issues, which reduces the cost of migration.

When moving applications and systems to the cloud, African FSPs should select a strategy based on their application landscape, integration requirements, the regulatory environment in which they operate, the availability of CSPs and the maturity of IT skills available[58].

In addition to adopting migration strategies, FSPs will need to choose a CSP that caters to their operational needs. Microsoft seems to be the preferred CSP for many African banks. Other CSPs that are being used by African banks are Amazon Web Services (AWS), IBM, SAP and Orange.

[58] Interviews with select African banks, Orange Business Services, 2019

2.8 CLOUD BANKING CASE STUDIES

A few international and African banks have already realised the value of cloud banking. This section explores some of the benefits that cloud banking has provided these banks.

WeBank, a subsidiary of Tencent, is China's first digital bank that is based in a private cloud and uses innovative technologies, such as AI and blockchain, to effect an extraordinary high volume of transactions at a very low cost[59]. The bank's operations are mainly driven by technology and innovation, where over half of all employees work in IT. By adopting a digital platform, WeBank has been able to run at 95% lower cost than that of traditional banks' IT operations. For example, the bank's digital platform enables it to make use of technologies like a chatbot, which handles 98% of customer queries and also collects applicant data, runs credit checks and nudges customers to make payments. The use of a chatbot significantly reduces the need to have a large number of staff in call centres to deal with customer queries.

The significant cut in operational costs has allowed the bank to pass these savings to their customers: the average cost for a WeBank customer per account per annum is USD 0.50 compared with the cost of between USD 3 - USD 15 per annum for an account with a traditional bank[60].

Cloud has also enabled WeBank to reduce its time-to-market significantly; it takes only two days to rapidly scale-out and 11 days to take a product to market[61]. The bank is also able to make rapid loan applications and real-time transaction settlements due to the flexibility and agility of the cloud.

N26, a Berlin-based digital bank, has leveraged cloud infrastructure and technology to launch a digital business model[62] where the bank can operate on a lower cost base by minimising IT resource requirements, as reflected in a smaller banking staff size.

Previously, only banks with deep pockets could invest and benefit from AI. Cloud can provide AI as a service where there is no need for banks to build their own AI systems, giving more banks access to artificial intelligence at a lower cost. Cloud also has the data storage capacity and processing capability

[59] A bank that runs accounts for just 50 cents a year, C. Skinner, 2019
[60] A bank that runs accounts for just 50 cents a year, C. Skinner, 2019
[61] WeBank: Digital Banking Decoded, WeBank, 2019
[62] N26 will bring successful European Digital Banking platform to the US, Forbes, 2019

that help enable AI innovation quickly. Operating on a cloud platform has provided access to AI technology for N26 and this has enabled it to adopt a customer-centric approach where customers' changing needs are met. The bank uses Mambu's SaaS banking engine that enables the integration of systems and quickly brings services to market in support of its growth strategy[63], where the bank has had a customer sign-up rate of up to 2,000 customers per day[64].

In Africa a number of new banks have combined a focus on a digital front end with a more virtual cloud back end.

TymeBank, a new digital entrant to the South African banking sector, has made a 56% cost saving by using cloud services from AWS rather than adopting traditional database technology[65]. Cloud has also allowed the bank to securely scale to support over 5,000 new customers a day since February 2019.

By having its back office in the cloud, TymeBank has a major cost advantage over competitors and has been able to pass cost savings to customers by providing cheaper banking services, allowing it to reach more of the under-served and unbanked market. This has also placed pressure on traditional banks to cut their fees to remain competitive: Capitec cut its Global One account monthly fees to USD 0.33; Nedbank cut the monthly account fee on its Pay-As-You-Use account to USD 0.36[66]; Standard Bank cut the MyMo account monthly fee to USD 0.33; and FNB cut its Easy Pay As-You-Use monthly account fees to USD 0.33[67].

TymeBank's use of APIs through its cloud banking platform allows it to connect with third-party partner systems and offer a richer customer value proposition, such as its partnership with a large supermarket chain in South Africa, Pick n Pay[68]. The bank's customers will be able to utilise any of the 14,000 Pick n Pay till points across the country to conduct their everyday banking transactions. The partnership also allows customers to earn extra Pick n Pay loyalty points when using their TymeBank card[69].

Bank Zero, another new digital bank in South Africa, is using IBM's cloud banking platform to provide app-driven banking services that offer low-cost transactions to consumers. The bank will also offer an all-digital cheque account that provides real-time account-checking, giving the customer full control of their money[70]. The app-based banking model allows customers to carry out a variety of banking transactions without physically going to the bank and is designed to handle customers' changing expectations of banking services[71].

Traditional banks across Africa are also starting to realise the value of cloud in improving the capabilities and costs of their operations. In particular, cloud computing should enable smaller African banks to resolve traditional challenges such as hiring quality IT staff and dealing with power outages[72].

The Islamic Bank of West Africa, a tier-three bank that serves approximately 125,500 customers[73] across four West African countries, launched a cloud-adoption programme in early 2019. Within the new programme critical applications will remain hosted on-premise in a traditional IT environment and backup applications such as mobile banking and ATMs will reside on a private cloud. The bank is expecting

[63] Mambu's SaaS Banking Engine Helps N26 Transform Operations, Mambu, 2017
[64] Mobile bank N26 sees customers tripling with two years: CEO, Reuters, 2017
[65] Amazon data centre chief lifts lid on SA plans, A. Goldstuck, 2019
[66] Year of the digital bank, Brainstorm: the Business Technology Magazine, 2019
[67] Digital newcomers spark price war among SA banks, ITWeb, 2019
[68] Year of the digital bank, Brainstorm: the Business Technology Magazine, 2019
[69] The battle of the banks, Mail & Guardian, 2019
[70] Year of the digital bank, Brainstorm: the Business Technology Magazine, 2019
[71] IBM to deliver digital banking platform for Bank Zero, IOL Business, 2018
[72] Interviews with select African banks, Orange Business Services, 2019
[73] Key figures, Tamweel Africa Holding website, 2017

significant cost savings from cloud banking: “Cloud technology allows us to reduce capex and opex, which allows us to offer banking services at a lower cost and enables faster time to market.”[74] The bank had prepared a business case that compared the cost of traditional on-premise solutions with cloud solutions and found that migrating to the cloud would provide a better return on investment to the bank by saving 15-20%. Significant cost savings are expected by cutting out hardware investments and lowering power-consumption costs. The estimated spending on cloud services in the upcoming years is around 10% of the bank’s current IT budget[72].

For larger African banks, cloud computing is seen as a strategic option to create business agility and reduce time to market for new banking solutions[72].

Banque du Caire, a tier-two bank that serves approximately 2.9 million customers in Egypt[75], has implemented cloud technology to enable the bank to enhance customer experience by taking innovative financial products to market quickly. Implementing cloud has also allowed the bank to transform its operations faster and has resulted in a significant reduction in overall costs.

Standard Bank has chosen AWS as its preferred CSP to migrate all production workloads for customer-facing platforms and strategic core banking platforms to the cloud[76]. AWS will also provide Standard Bank with machine-learning and analytics services that will enable the bank to build more advanced fraud-detection systems and create innovative financial products that cater to customers’ evolving needs. The borderless nature of the cloud will also allow Standard Bank’s pan-African operations to more easily integrate their services and improve accessibility irrespective of location.

The transformation to cloud banking in Africa is still in its infancy. In 2019 global players such as Amazon and Microsoft will open their first data centres on the continent. This will improve cloud services and be able to support both large and small banks to move towards cloud strategies[77]. In addition to stimulating economic development for customers and partners, local data centre infrastructure enables companies, governments and regulated industries to realise the benefits of the cloud for digital transformation and strengthens the technology ecosystem that supports digital transformation[78]. Local data centres also address some of the issues of data sovereignty and network latency that were holding some banks back from implementing cloud computing[79].

We are beginning to see instances of local cloud providers emerging. Liquid Telecom is a leading pan-African telecoms and cloud services provider with a footprint of data centres across the continent (including Nairobi, Harare and Kigali). Liquid Telecom is facilitating the growth of Africa’s cloud by providing a platform for cloud services to be delivered locally in many markets for the first time. In December 2018, the company announced it will invest USD 400 million in network connectivity and data centres in Egypt. The network connects over 13 countries on the continent.

[74] Interviews with select African banks, Orange Business Services, 2019
[75] Banque du Caire goes live with Temenos to re-define digital customer experience, Temenos, 2019
[76] Amazon data centre chief lifts lid on SA plans, A. Goldstuck, 2019
[77] Interviews with select African banks, Orange Business Services, 2019
[78] Cloud computing grows in SA, T. Shapshak, 2019
[79] SA set to embrace the public cloud, DUO Marketing, 2019

Part 3

REGULATION

REGULATION

3.1 INTRODUCTION

This chapter investigates how regulators are engaging with technology and innovation in financial services. It analyses international best practices on the regulation of cloud banking in order to inform the proposed model for regulation in Africa that is discussed in the next chapter.

From a traditional regulatory standpoint, cloud banking contracts would most often qualify as an outsourcing agreement of essential services. Most supervisory authorities are now developing detailed positions on the outsourcing of essential services. In particular, cloud computing requires regulators to have clear positions on a number of policy areas:

- **Data privacy:** The success of cloud computing depends on whether users believe that their data is being protected and used in a transparent manner. In order to obtain the maximum benefit that cloud solutions present, CSPs need to be able to freely move data through the cloud in the most efficient way, which can involve cross-border movement of data. As a result regulators need to ensure that there are adequate privacy laws in place in whatever jurisdiction data resides[80].

- **Data risk and security:** Cloud solutions are typically delivered through physical servers that sit outside the financial service providers' own infrastructure (and may sit in other jurisdictions) and are owned and controlled by third-party CSPs. This is not necessarily a risk because many large CSPs understand that security is at the core of their business and invest accordingly, and may have more secure IT infrastructures than many financial institutions (especially the smaller institutions in Africa). Nonetheless, in allowing a financial institution to engage with a CSP, the regulator needs to define clear rules with respect to encryption and data-access controls, how to ensure confidentiality, and prevent leakage and ensure the integrity and preservation of the data, especially in multi-tenancy or shared infrastructure models.

- **Cybercrime:** Data stored on computer networks is not only vulnerable to general data security risks, such as data leakage, but also cybercrime. Regulators need to ensure that there are legislative, investigative and enforcement tools available to protect data subjects and data holders from cyber criminals. This involves creating and implementing cybercrime laws that protect data stored in the cloud from cyberattacks and unauthorised access, and ensure that such laws exist in any jurisdiction in which the CSP operates[80].

- **Data sovereignty:** Many of the benefits of cloud rest on the economies of scale achieved through storing and processing of large data estates. Requirements to host data within a certain country necessitates the building of infrastructure required to store and process that data. Even the largest cloud providers and users do not maintain data centres in every jurisdiction in which they operate – and this is most certainly the case in the smaller countries in Africa. Policies that require data to be stored and processed locally may be an attempt to protect jobs or concerns about international interference in domestic entities, but this will increase the cost of providing financial services. Regulators need to balance the benefits of scale against any such policy concerns.

- **Protection of intellectual property:** CSPs rely on a combination of patents, copyrights and other forms of intellectual property protection to produce innovative cloud solutions. If a country is to benefit

[80] BSA Global Cloud Computing Scorecard, BSA, 2018

from such services, national authorities need to implement intellectual property laws that provide clear protection and enforcement against misappropriation and infringement of the technology developments of cloud solutions[81].

- **Vendor risk:** The reliance on a limited number of service providers presents a concentration risk. If a major CSP experienced a disruption in service it has the potential to disrupt a number of institutions in the market. Regulators need to ensure that CSPs have adequate controls in place to comply with various laws, rules and regulations on disaster recovery and service levels, and that all their third-party providers comply with the same laws, rules and regulations.

- **Support for industry-led standards and international harmonisation of rules:** Restrictive policies such as tariffs and trade barriers on cross-border services inhibit the use of cloud services. There needs to be harmonisation efforts between regulators to develop international standards that will ensure optimal portability, allow CSPs to operate free from trade barriers, and minimise conflicting legal obligations on CSPs[81].

- **ICT readiness and broadband deployment:** Cloud computing requires extensive and affordable broadband access. In order to achieve an adequate level of ICT infrastructure to support cloud-computing access, national telecommunications authorities need to implement policies that incentivise investment in broadband infrastructure and laws that ensure there is universal access to broadband networks.

- **Migration complexity and operational risk**: Regulators need to ensure a financial institutions' resilience in the wake of a disruption to cloud services.

Different regulators have adopted a range of approaches to the regulation of cloud banking – from passive or reactive to proactive regulation. Passive regulators do not take an upfront position but rather allow the market to develop, monitor innovation and intervene when risks are identified or an issue arises. Regulators following this approach allow the market to innovate without restriction. However, this freedom has some drawbacks. First, there is a level of risk that could potentially go unchecked and threaten the stability of the market. Second, the regulatory ambiguity can hinder innovation as firms are unwilling to take the risk of investing in innovation that could be later opposed by a regulator. Regulatory arbitrage is also more likely under a passive regulator because new entrants are able to participate in the financial services sector without falling under that same strict regulatory codes as incumbent institutions[82]. An effective proactive regulatory approach requires a close working relationship between innovators and regulators, enabling regulators to understand new developments and create an enabling regulatory framework, rather than acting as a block on innovation.

Increasingly, government agencies are working with financial sector regulators to facilitate engagement with innovators and developing a supportive ecosystem to encourage innovation within a market:

- **Innovation hubs** provide support to startups that struggle to navigate the complex regulations imposed on the financial services sector, by giving them access to regulators and providing guidance on the regulatory application process. These hubs can also provide additional resources such as communal working spaces, datasets, expertise in entrepreneurship, as well as assisting businesses with finding commercial funding opportunities[83].

[81] BSA Global Cloud Computing Scorecard, BSA, 2018

[82] This is a charge often applied to the providers of mobile money who face a lower level of regulation that banks.

[83] The impact of the 4th industrial revolution on South African financial services market, Centre of Excellence in Financial Services, 2017

- **Regulatory sandboxes** create live environments for innovators to test new products and services in a controlled environment[84]. Sandboxes allow regulators to understand the technology, assess any potential emerging risks and adjust regulation to adapt to the growth and pace of innovation. The use of sandboxes sends a clear message to the market that innovation is on the regulator's agenda[85].

- **Working groups** are often inter-regulatory groups that promote collaboration across regulators in their responses to innovation. Most working-group mandates involve assessing the implications, reviewing and appropriately revising regulatory frameworks to respond to the dynamics of rapidly changing technology.

3.2 INTERNATIONAL BEST PRACTICES ON CLOUD BANKING

The European Union has been at the forefront of defining an enabling regulatory environment for cloud banking services. This has involved both the regulation on the use of data and privacy (not specifically related to the financial sector), regulations to govern access to the payment system and financial sector specific guidelines

The General Data Protection Regulation (GDPR), implemented by the EU in 2018, provides a consistent and unified legal basis for data protection and enforcement across the EU. The regulation aims to define the regulatory environment for business so consumers and businesses in the EU can fully benefit from a digital economy. Under the regulations all institutions (including financial institutions) have to ensure that consumer personal data is gathered legally and under strict conditions, and that consumer data is fully protected. Failure to achieve GDPR compliance can result in stiff penalties and fines for both the affected institution and the CSPs. The fines can be up to 4% of the violating company's global annual revenue[86]. International companies that collect or process EU citizens' personal data is also subjected to the GDPR requirements and penalties.

Some of the key privacy and data protection requirements include requiring the consent of subjects for data processing, ensuring anonymity of collected data to protect privacy, providing data-breach notifications, and safely handling the transfer of data across borders[86].

Data-breach notifications are an important element of the GDPR regulation. Data controllers must notify regulators of personal data breaches within 72 hours of learning of these, as well as provide specific details of the breach, such as the nature of the breach and the number of data subjects affected[86]. Companies must also perform Data Protection Impact Assessments to identify any risks to consumer data that processing operations may present, especially those that use new technologies. In order to address any identified risks, companies are required to conduct compliance reviews of their data protection policies.

Some of the regulatory responsibility of the GDPR is shifted to CSPs, where these service providers will need to develop and implement a number of internal practices to protect citizens' personal data against loss or exposure, as well as have full processing transparency[87]. Regulators also have the right to hold financial institutions and CSPs responsible for not adhering to the principles of regulation. This will relieve some of the regulatory burden that financial institutions previously faced alone. In order to meet the GDPR requirements, financial institutions will need to evaluate the legitimacy of their data-processing operations by demonstrating their ability to restore and access personal data as well as implement appropriate controls

[84] What is a regulatory sandbox, BBVA, 2017
[85] Working paper: Regulatory sandboxes and financial inclusion, CGAP, 2017
[86] What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019, J. De Groot, 2019
[87] Turning the regulatory challenges of cloud into competitive advantage, IBM, 2017

such as disaster recovery procedures[87].

The second regulation that impacts the adoption of cloud banking services is the revised Payment Service Directive (PSD2) that aims to contribute to a more integrated and efficient European payments market. This creates a level playing field for payment service providers given the rise of fintechs, makes payments safer and more secure as well as ensures enhanced security and strong customer protection. PSD2 requires banks to provide third parties access to their customers' account data using APIs[88]. The Open Banking provisions allow non-banks, corporates or fintechs to directly access consumer bank accounts to perform payments activities and/or gain access to customer data.

FSPs in Europe are required to balance the strict data protection requirements of GDPR while still complying with open-banking provisions of PSD2[89]. In order to comply with PSD2 while still maintaining customer privacy, companies will need to set limits on what third parties can and cannot do. Customer permission, as well as duration and contextual limits, will determine the extent of third-party data sharing[90]. Third parties are also required to create functionality where customers are able to review and withdraw permissions at their discretion.

Under PSD2, financial institutions need to implement systems and processes that enable flexible data management to ensure that data is easily accessible and can be segregated because customers can ask to move their data to another FSP at any time. There should also be processes and audits in place that require third parties to handle data with consent of customers[90]. Financial institutions will also need to communicate in a simple and transparent manner when persuading customers to share personal data, as well as use encryption and data-masking techniques to mitigate risk. All of this is much easier to achieve when data is stored on, and accessed from, the cloud.

The European Banking Authority (EBA) released its final guidance for the use of CSPs by financial institutions at the end of 2017 that set out the regulator's expectations if financial institutions intend to adopt cloud computing services[91]. The recommendations address five key areas:

- **Security of data systems:** The CSP must protect the confidentiality of the information transmitted by the financial institution[92]. Institutions should conduct a thorough risk-based evaluation of activities, processes, and related data and systems that are to be outsourced to a cloud computing solution. Institutions need to also define and decide on an appropriate level of protection of data confidentiality, integrity and traceability of data, and systems in the context of the intended cloud outsourcing[92].

- **Access and audit rights:** The guidelines recognise the concept of materiality and require the financial institution to keep a register of material and non-material outsourced activities. Furthermore, financial institutions and regulators should have full access to the CSP business premises, unrestricted rights of inspection and audit related to the outsourced services[93].
- **Location of data and data processing:** The financial institution should adopt a risk-based approach in considering data storage and processing locations. The assessment should address the potential risk impacts, legal risks and compliance issues, and oversight limitation related to the countries where the outsourced services are or likely to be provided, and where data is, or is likely to be, stored. Wider political and security stability of the jurisdictions should also be taken into consideration[94].

[88] PSD2- a game changing regulation, PWC, 2018
[89] GDPR and Privacy Best Practices of Financial Services Firms, Forrester, 2017
[90] PSD2 – Are you ready to embrace the change?, PWC, 2017
[91] EBA issues guidance for the use of cloud service providers by financial institutions, European Banking Authority, 2017
[92] Recommendations on outsourcing to cloud providers, European Banking Authority, 2017
[93] How IBM supports banks in the context of the European Banking Authority recommendations on Cloud Computing, IBM, 2018
[94] Recommendations on outsourcing to cloud providers, European Banking Authority, 2017

- **Chain outsourcing:** Institutions should take account of the risks associated with chain outsourcing where the outsourcing service provider subcontracts elements of the service to other providers[94].
- **Contingency plans and exit strategies:** Institutions should plan and implement arrangements to maintain the continuity of their business in the event that the provision of services by an outsourcing service provider fails, or deteriorates to an unacceptable degree. The policy should include contingency planning and a clearly defined exit strategy. Institutions should also ensure that they are able to exit cloud outsourcing arrangements if needed without undue disruption to their provision of services, or adverse effects on their compliance with the regulatory regime and without detriment to the continuity and quality of its provision of services to clients[93].

Within the EU individual countries retain their own banking sector regulator, who needs to implement some version of these guidelines. Accordingly BaFin, the financial regulatory authority in **Germany**, has taken steps to clarify and specify the regulatory framework for cloud computing in Germany. The framework must comply with the outsourcing requirements of the German Banking Act, which requires that banks must make appropriate arrangements to avoid excessive additional risks when outsourcing services or activities to third parties[95]. Further, BaFin has the right to review and audit the banks' outsourcing agreements with CSPs. If the cloud service is a material outsourcing arrangement, then it is required to be evaluated case by case[96].

In the EU, banking regulators are able to leverage the extensive data protection legislation that has been created by the GDPR. The data protection legislation states that CSPs must implement technical and organisational measures to ensure the security of data[97]. There are also data security and security breach notification obligations imposed onto CSPs.

The Bank of England (BoE) has also identified priority areas for action by the BoE around innovation and technology, stating that it will encourage innovation between FSPs to support the emergence of a new financial system that can meet the needs of a new economy. More specifically, the BoE has stated that it is prioritising cloud adoption and will facilitate financial institutions' use of cloud technology to increase their operational resilience. The BoE plans to publish a supervisory statement that will outline the Prudential Regulation Authority's (PRA) modernised policy framework on outsourcing arrangements, including a focus on cloud computing and setting out conditions that can help give financial institutions assurance on its use[98]. The BoE will also establish a working group with the Financial Conduct Authority, and public and private companies to explore what principles and guidance could support safe adoption of cloud[98].

In contrast to Europe, the **United States** does not have a single unified federal data privacy law in place. There are various sources of responsibility and standards for data privacy in the form of bank regulator guidance, state laws, case law and industry standards. Privacy protection in the financial services sector is governed by strong sectoral laws[99]. The US does have financial sector-specific security requirements that require financial institutions to encrypt data and take steps to identify identity fraud. However, some states have stricter requirements than others. There are no specific enforceable security audit requirements in place for financial institutions, which is particularly important for regulating cloud computing. Most security issues are dealt with by consumer law where companies are held accountable to consumers for using and storing their data securely and keeping data confidential[99].

The Federal Trade Commission Fair Information Practice has formed a set of guidelines concerning the

[95] Banking Act, Deutsche Bundesbank, 2014

[96] German Federal Financial Supervisory Authority Publishes Guidance on the Regulatory Framework for Cloud Services, The National Law Review, 2018

[97] Country Report: Germany, 2018

[98] The Bank of England's response to the Van Steenis review on the Future of Finance, Bank of England, 2019

[99] Country Report: The United States, BSA, 2018

fair use of confidential information[100]. Although the guidelines do not specifically address cloud computing, there are five principles that can be applied to regulate cloud computing. The first principle states that *consumers should be given notice* that their data is being collected and processed and they should be provided with details of who is using the information and how the data processor will ensure the confidentiality, quality and integrity of the data. Second, consumers will also have the *right to decide on how their information is used* and whether it can be passed on to third parties. The third principle states that *consumers should be able to access and alter their data* and be able to correct any mistakes regarding their information. The fourth principle states that *financial institutions should ensure the integrity and security of all data*. The financial institution shoulders the responsibility of ensuring that the information is accurate as well as ensuring that there are sufficient safeguards in place to protect data from cyberattacks. The final principle states that there needs to be *mechanisms for enforcement of the above practices*, i.e. regulators and supervisory authorities.

In 2012, the Federal Financial Institutions Examination Council (FFIEC) issued a statement advising that financial institutions undertake a thorough due diligence and risk assessment for outsourced cloud computing arrangements[101]. The FFIEC statement emphasises six key elements: due diligence; vendor management; auditing; information security; legal, regulatory and reputational considerations; and business continuity planning.

With regard to due diligence, the FFIEC identifies a number of issues with outsourcing to the cloud, namely: data classification, data segregation and data recoverability. In order to mitigate these risks, financial institutions should implement various security controls, such as: maintain a comprehensive data inventory and suitable data classification process; appropriate access restrictions to customer data through identity and access management; monitor security-related threats on financial institutions' and CSPs' networks; and comprehensive incident response methodologies as well as forensic strategies for auditing and investigation purposes[102].

Financial institutions also need to undertake vendor management when entering outsourced cloud computing arrangements. This includes verifying the CSPs' data handling processes, the adequacy and availability of backup data as well as whether CSPs share cloud facilities. CSPs that use multi-tenant deployments will need to increase data protection through encryption and assurances that proper controls are in place so data is not leaked between tenants. Additional factors, such as ownership, location and format of data, dispute resolution, the removal of data after the contract has expired, and the CSP's obligations with regard to financial institutions' responsibilities for compliance with privacy laws need to be addressed in outsourced cloud computing agreements[103].

The FFIEC also requires financial institutions to identify, mitigate and understand legal, regulatory and reputational risks, even though assessing compliance might be more complex in an environment where the CSP processes and stores data in another jurisdiction.

Federal banking regulators are starting to take a more active approach in overseeing the use of cloud within the financial sector in the US. One of the Federal Reserve's initiatives is to exercise established governance and procurement protocols, support active usage, and enhance the architecture of the innovation lab by evaluating cloud-based services offerings[104]. In April 2019, Federal Reserve authorities

[100] Cloud computing and privacy regulations: an exploratory study on issues and implications, M. AlSudiari, T. Vasista, 2012
[101] Moving to the Cloud- The Intersection of Cloud Computing, Financial Services and Regulation in Europe, the United Kingdom and the United States, D. Milanesi, 2018
[102] Moving to the Cloud- The Intersection of Cloud Computing, Financial Services and Regulation in Europe, the United Kingdom and the United States, D. Milanesi, 2018
[103] Moving to the Cloud- The Intersection of Cloud Computing, Financial Services and Regulation in Europe, the United Kingdom and the United States, D. Milanesi, 2018
[104] Annual Performance Report 2018, Board of Governors of the Federal Reserve System, 2019

examined AWS' resiliency and backup systems as part of ongoing oversight of the company's cloud services to banks[105].

Other developing markets have also taken steps to regulate cloud computing.

Turkey has released financial sector regulations that leverage the strong data protection regulation regime that has been implemented and is based on the EU Data Protection Directive, which has ensured that it is comprehensive in scope as well as compatible with international standards[106]. The Data Protection Law obliges CSPs to take appropriate technical and administrative measures to protect confidential information. However, the law does not specify these requirements. Where there is a third party involved in the data processing, the responsibility of data security is shared with the third party and the institution outsourcing this service.

The Data Protection Law also provides key principles to be followed with regard to processing data. Financial institutions or third parties must have a *transparent process* where the process, purpose and scope of processing data must be clear, well informed and easy to understand[107]. The data must be *processed for specific and legitimate purposes* and the processing of data must be relevant and necessary for these purposes. Further*, personal data must be retained for the period of time stipulated by regulation*, depending on the purpose of processing. In the case of data security breaches, data controllers have to *notify both the data subject as well as Personal Data Protection Board* of the breach as soon as possible.

Individuals will have the right to access their data and obtain copies of their data, as well as understand the purpose of processing their data. The regulation also gives individuals the right to request the data processor to delete their data and object to having their data processed[108].

The Turkish Banking Regulation and Supervision Agency (BRSA) released a draft regulation on the Information Systems of the Banks and Electronic Banking Services in 2018. The draft regulation sets the standards for the management of information systems used for banking activities and regulates the minimum procedures to be implemented for the security of these systems[109]. The board of directors at the bank is obligated to ensure that the security measures related to ICT systems are sufficient. Banks must also take measures to ensure that the privacy of data is always maintained whenever it is moved, transferred, processed, stored or preserved. Banks must implement reliable encryption techniques as well as use end-to-end secure communication to transfer data for security purposes[109].

The draft regulation also states that a bank may use cloud services if the service provider specifically delivers services to banks and the cloud deployment model complies with the banking regulations[109]. Banks are allowed to use collective cloud services for some core banking applications if they get permission from BRSA. Banks will also need to obtain explicit consent from consumers regarding transferring personal data to third parties as well as transferring data across borders[110].

The BRSA's draft regulation, as well as the new Data Protection Law, have created an environment to encourage the development of cloud banking in Turkey. Microsoft announced in 2018 that it is actively trying to spread the use of cloud computing in Turkey[111]. DenizBank, a Turkish bank with an asset base of USD 37 billion, uses cloud to host its digital banking platform. According to Microsoft, it has saved DenizBank USD 12 million in data centre costs by migrating some of its systems to Microsoft's private

[105] U.S. banking regulators examined Amazon's cloud in April: WSJ, Reuters, 2019
[106] Country Report: Turkey, BSA, 2018
[107] Turkey: Data Protection 2018, E. Firat & D. Alkan, 2018
[108] Turkey: Data Protection 2018, E. Firat & D. Alkan, 2018
[109] Turkey: Draft regulation on the information systems of the banks and electronic banking services, CMS Law-Now, 2019
[110] Using the cloud under the Turkish data protection law, O. Karaduman, 2017
[111] Microsoft targets to spread cloud computing in Turkey: Country chief, Hurriyet Daily News, 2018

cloud[112].

Yapi Kredi, one of Turkey's largest banks with an asset base of USD 70.4 billion[113], carried out a virtualisation initiative in 2011 where applications and activities such as website hosting, database management, extranet servers and credit-card transaction servers were moved to secure virtual servers. The virtualisation of these servers was seen as vital in ensuring that the future transition to the cloud environment will be a smooth one[114]. According to its 2018 annual report, Yapi Kredi has begun using corporate cloud, which aligns with the release of the new Data Protection Law as well as the BRSA draft regulation.

Another developing country where the legal and regulatory environment for cloud banking is well advanced is **Argentina**.

In order to gain a better understanding of cloud services, the Central Bank of Argentina (BCRA) created a technological innovation unit to study the approaches of other central banks where the best international practices are analysed and applied to the BCRA's context[115]. As a result of its understanding of the cloud environment, the BCRA now allows banks to outsource their services to the cloud, which was previously prohibited.

The bank regulator was able to leverage the work of other regulators that had created a solid environment for data protection. Argentina has progressed substantially in data protection laws and continues to update aspects of the law. The Personal Data Protection Law (PDPL) follows international standards, specifically the EU framework, and has been considered by the European Commission as granting adequate protection. This would allow a firm in Argentina to offer services to Europe since it upholds the same standard of data protection. There are also effective cybercrime laws in place that cover all the main cybercrime categories that relate to cloud computing. The cybercrime legislation is also consistent with the EU Convention on Cybercrime.

The PDPL states the collection and processing of data must be authorised by the data subject. The data subject must also be informed about the purpose for which the data is to be processed and who will have access to the data. The data subject has the right to access, rectify and delete its data from the data processor's system at any point. In the case of transferring data to third parties, particularly relevant to cloud computing, personal data may only be transferred for legitimate purposes and the data subject must give consent.

Furthermore, cross-border transfer of personal data is prohibited to countries that do not have adequate data protection laws, unless the data subject consents to the transfer, or there is adequate protection through the contractual clauses from the third-party CSP[116]. This requirement does not apply when the transfer of data is necessary for international judicial cooperation. Then the transfer takes place as provided for in the context of international treaties to which Argentina is party to, or the transfer has as its purpose the international cooperation between intelligence agencies engaged in combating organised crime[117].

With regard to data security, Argentine law requires that the organisation responsible for processing and storing personal data must adopt the technical and organisational measures to ensure the security and confidentiality of personal data. Data security-breach notifications are not specifically required under PDPL, but failure to notify the data protection authority may impact other security violations if the failure to notify

[112] Enable application management for the cloud era, Microsoft, 2013
[113] Banks' annual report data, BankFocus, 2018
[114] Turkish Bank Confidently Embraces Virtualization, Trend Micro, 2011
[115] Financial innovation, Banco Central de la Republica Argentina, 2018
[116] Data Protection & Privacy Argentina, D. Fernandez, 2018
[117] Data Protection Laws of the World: Argentina, DLA Piper, 2019

results in other security breaches. The organisation processing and storing the data must keep records of security breaches because the data protection authority may request these records[117].

Since Argentine banks have been given the green light for cloud banking, traditional banks are starting to adopt cloud banking, partly to compete against new digital entrants[118]. Banco Macro, Argentina's largest domestically-owned private bank, has launched a new business loans entity (Alumbra) for microenterprises and small businesses on a cloud platform called Mambu. Alumbra aims to promote greater financial inclusion by offering loans to small businesses and microenterprises in underserved markets such as Salta, which is one of Argentina's poorest regions[119]. ICBC Argentina has also realised the value of cloud and signed a five-year USD 63 million agreement with IBM for AI and cloud services in February 2019[120].

3.3. AFRICA'S FINANCIAL SECTOR REGULATORY APPROACH

African financial sector regulators' approaches to cloud banking vary considerably. Besides South Africa, few African financial sector regulators have taken a definitive stance on cloud banking, or proposed a guiding regulatory framework. Some financial sector regulators have implemented legislation that covers different aspects of outsourcing and offshoring of data, operations (people) and processing, in a manner that retards the adoption of cloud banking.

Some African financial regulators have not overreacted to new technologies, to avoid inhibiting innovation. This is evident in the case of M-Pesa in Kenya, where the regulator allowed Safaricom to pursue mobile money despite a lack of regulation on the use of the technology. The regulator adopted a wait-and-see approach to mobile money and once M-Pesa had developed to a certain degree, it implemented a regulatory framework for mobile money in Kenya.

Other African financial regulators have taken a more proactive approach. The Central Bank of **Nigeria** (CBN) prohibits the use of innovative technologies until the Central Bank has a clear understanding of the risks and benefits. The Central Bank of Nigeria has an inter-departmental committee designing a framework for open banking that is largely based on the EU PSD2 regulation[121]. The objective of the Nigeria Open Banking initiative is to analyse the need of the industry for common API standards among banks and other financial institutions; develop common API standards; provide a regulatory sandbox and other testing tools for certification; promote adoption of open banking standards with stakeholders across Nigeria; and enable further innovation in the financial services industry[122]. Until this framework for cloud banking is approved and implemented by the regulator, financial institutions are restricted in using cloud banking platforms.

The **South African** Reserve Bank (SARB) is another central bank that takes a proactive regulatory approach and issued a directive regarding cloud computing and the offshoring of data in 2018. Under this directive banks are required to follow a risk-based approach when adopting cloud solutions[123]. The directive states that different cloud models implemented by banks should be assessed based on the level of risk and whether risk mitigation controls are managed internally, externally and/or through a combination of both. The SARB directive requires banks to have a formally defined and board approved data strategy and

[118] Argentine Banks: Time to Innovate, BBVA, 2017

[119] Mambu Helps Argentina's Banco Macro Reach Small Business And Microenterprise Customers, Mambu, 2014

[120] ICBC Argentina Strikes a $63M Services Agreement with IBM to Reimagine Customer Services in Argentinian Banking Industry with AI and Cloud, IBM, 2019

[121] Nigeria: Fintechs ,Banks Await Regulation on Open Banking, U. Aliogo, 2018

[122] Open Banking Nigeria website, 2019

[123] Directive on cloud computing, the South African Reserve Bank, 2018

data governance framework that clearly defines policies for cloud computing. Banks must also take all reasonable measures to ensure the confidentiality, integrity and availability of personal data that is processed via the cloud. If banks use third parties for cloud services, they must ensure that the third parties adhere to the information-security requirements that have been defined by the bank[123].

Although other central banks in the SADC region have not yet issued explicit directives on cloud banking, some have released outsourcing guidelines that would cover cloud computing contracts. The Bank of **Zambia** (BoZ), for instance, prohibits banks from outsourcing core management functions, such as corporate planning, organisation, management and control, and decision-making and risk management functions[124]. It is unclear how this would affect banks that have personnel in country who rely on cloud-based systems and solutions, and could certainly be considered a constraint to the operations of some international banks. In addition, offshoring banking activities to different jurisdictions requires approval from the BoZ as it exposes the bank to country risk that may adversely affect the bank.

In countries where there is a lack of strong general regulation around topics that implement cloud, such as data protection and outsourcing laws, central banks need to embed such regulation within their guidelines.

An example of central banks acting in proxy for general regulation is the Central Bank of **Kenya** (CBK). The CBK requires that Kenyan banks have outsourcing policies that directly affect cloud banking. The policies encompass the procedures for determining whether and how activities can be outsourced; the sound structuring of the outsourcing agreement, including ownership and confidentiality of data; programmes for managing and monitoring the risks associated with outsourcing; and the establishment of an effective control environment at the bank and service provider[125]. Banks cannot outsource core management functions such as corporate planning, organisation, management and control, and decision-making functions like decisions to grant loans. Banks that plan to outsource material activities to third parties such as information system management and maintenance, i.e. data entry processing, data centres, facilities management, and end-user support, will require approval from the CBK[126].

In addition, the offshoring of data or banking activities to third parties based in overseas jurisdictions must be approved by the CBK. The offshore outsourcing arrangements should only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements[126]. The CBK requires that it should have unrestricted access to the information from the overseas regulator.

Despite currently having no formal legal frameworks or policies in place with regard to fintech innovation, the CBK has taken the initiative to provide guidance and take an open-minded approach towards fintech innovations by allowing fintech companies to partner with platform providers to develop financial services applications that operate on open banking principles[127]. The CBK has also published a guidance note that outlines the minimum requirements that financial institutions should build on in the development and implementation of strategies, policies, procedures and related activities aimed at mitigating cyber risk and promote stability of the Kenyan banking sector[128].

The East African Community (EAC) has adopted a modern and effective regionally harmonised framework for cyber laws[129]. Phase one of the framework covers electronic transactions, electronic signatures and authentication, cybercrime and data protection, and privacy. However, the implementation of e-commerce legislation that includes data privacy and cybercrime legislation has yet to be promulgated.

---

[124] Gazette Notice No. 717 of 2014, Bank of Zambia, 2014
[125] Risk Management Guidelines, Central Bank of Kenya, 2013
[126] Prudential Guidelines, Central Bank of Kenya, 2013
[127] Open Banking in Africa- the power of data, Hogan Lovells, 2018
[128] Guidance note on cybersecurity, Central Bank of Kenya, 2017
[129] Harmonizing Cyberlaws and Regulations: The experience of the East African Community, UNCTAD, 2012

The National Bank of **Rwanda** (BNR) has been more progressive in its regulatory approach to innovation. For instance, it has modelled some regulation based on the EU's PSD2 regulation. The legislation makes provisions for new types of payments providers and the implementation of a regulatory sandbox to test innovative digital products[127]. The regulatory sandbox will allow innovators in digital finance to easily enter the market as well as enable the BNR to monitor developments that will inform decisions on how to best regulate innovation in the future[130]. Riha Payment System is the first startup to be granted permission to test its innovative mobile wallet solution in the BNR's regulatory sandbox[131].

Although the BNR has not directly stipulated how this regulation will affect cloud computing, based on the fact that regulation has been modelled on the EU's PSD2 regulation, which requires banks to provide data to third parties using APIs, it could be assumed that the BNR will have an enabling approach to cloud banking.

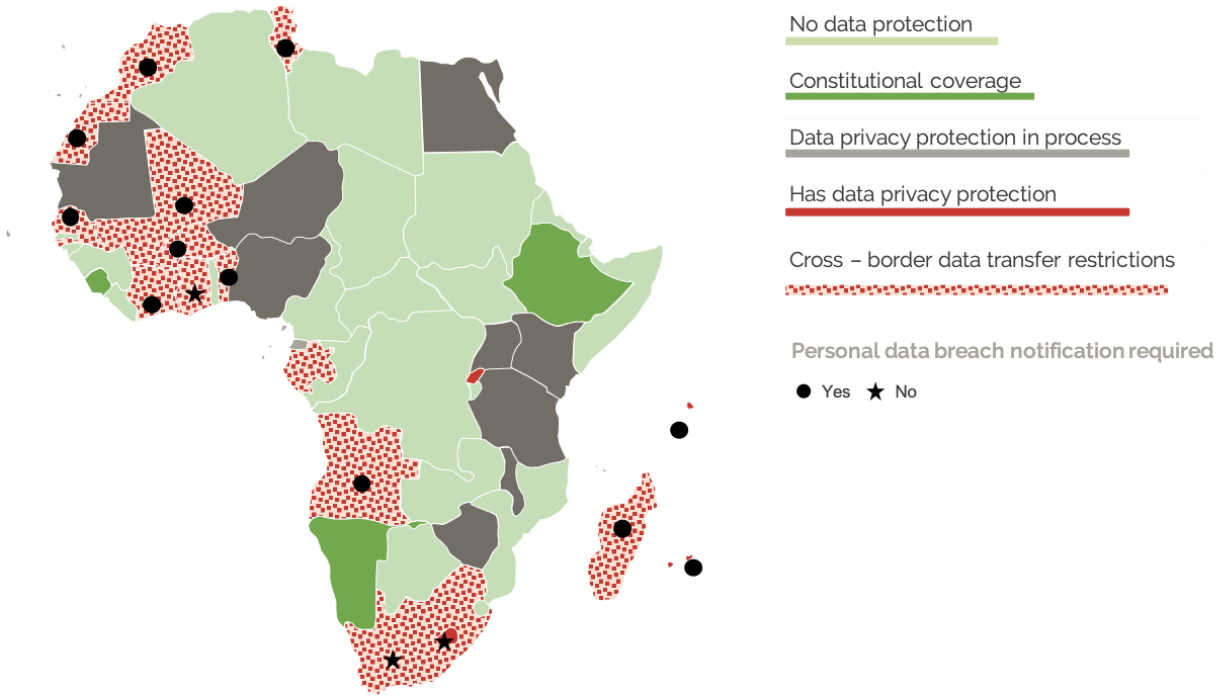
In order for financial institutions to use cloud banking technologies from CSPs within their own countries, the regulator needs to ensure that there are appropriate data protection rules in the country or to develop rules under its banking regulations. If financial institutions plan to use cloud banking platforms based in other countries, the regulator needs to ensure that such services are provided from countries with strong data protection laws. Approximately 29% of African countries have data privacy legislation in place[132] and this means that financial regulators will need to compensate with strong sectoral laws for weak general data protection laws.

Furthermore, there needs to be a balance between data protection and safeguarding the right of access to information because in some cases data protection laws can disregard consumers' rights. In Tunisia, public organisations do not have to declare data processing and could deprive individuals of the possibility to exercise their rights of access, rectification and to express their informed consent[133]. Similarly, cybercrime and data protection laws in Egypt use vague language to identify crimes that put consumer rights at risk under the pretext of countering threats to security[134].

Rather than a blanket restriction on moving data offshore, which may drive up the cost of banking solutions, regulators need to define strong cross-border data rules that link any cross-border data movement to the quality protection in the receiving country. As figure 3.1 shows, the few African countries that have data privacy-protection regulation in place also restrict cross-border data transfers, which will be a major inhibitor of future cloud usage. These legislative disparities across the continent make it challenging for multinational organisations to share data across the continent and globally.

[130] John RwangombwaL Delivering Rwanda's digital-driven economy, where everyone is a winner, The Banker, 2019
[131] Rwanda: Central Bank grants testing approval to emerging fintech firm, MobileMoneyAfrica, 2018
[132] Privacy is Paramount – Personal Data Protection in Africa, Deloitte, 2017
[133] Data protection in Tunisia: a legal illusion?, Centre for Internet and Human Rights, 2018
[134] North Africa should fight online crime the right way, Enact, 2019

Figure 3.1. Africa personal data protection regulatory landscape[135]



For those that do have legislation in place, the rules for data sharing are not uniform and are based on outdated principles that are largely consistent with the EU's previous directive that GDPR will replace[136].

The SADC Model Law on Data Protection sets rules on the processing of personal data, duties of data controllers and data processors, and stipulates the rights of the data subject. The model law states that the data controller should ensure that processed personal data is accurate as well as relevant to the purposes for which it is collected. In addition to this, data subjects have the right to access, correct and delete their information at their discretion. The Model Law on Data Protection states that data controllers must ensure that personal data that is processed should be accessible, regardless of the technology, and ensure that the evolution of technology will not become an obstacle in processing personal data securely[137]. If there is a data security breach, the data controller/processor must notify the regulator immediately.

The SADC Model Law on Cybercrime also provides additional protection for financial institutions against cyberattacks on the confidentiality, integrity and availability of data and systems. There are also cross-border rules where personal data can only be transferred if there are adequate data protection measures in place in the recipient country.

The West African region is one of the more developed regions in Africa when it comes to regulation of e-commerce. The Economic Community of West African States (ECOWAS) has adopted several regulatory frameworks that govern e-commerce with the aim of creating a harmonised legal environment in the area of e-transactions, data protection and cybercrime[138]. The majority of countries have adopted legislation on electronic transactions and have taken steps towards the implementation of the Supplementary Act on Personal Data Protection. The Act requires countries to outline a legal framework for the protection of

[135] *Source: Privacy is Paramount – Personal Data Protection in Africa, Deloitte, 2017*
[136] Data privacy in Africa: Regulation and reality, K. Kuhlcke, 2017
[137] Southern African Development Community Model Law: Data Protection, HIPSSA, 2013
[138] Review of e-commerce legislation harmonization in the Economic Community of West African States, UNCTAD, 2015

personal data, set standards for the processing of personal data, establish an institutional base, define the rights of interested parties and clarify obligations of those responsible for personal data processing.

In conclusion, the regulatory approach to cloud banking differs widely across Africa[139] and needs to address the specific challenges created by the level of effective data and e-commerce regulation in each region. The next section sets out some recommendations on the way forward.

[139] This was also confirmed in meetings with central banks and financial sector regulators conducted for this study. For a list of regulators who participated see footnote 2.

Part 4

A NEW MODEL OF REGULATION

A NEW MODEL OF REGULATION

This chapter proposes a model for regulation that can be adopted across the African continent given the best international practices and regulatory frameworks outlined in the previous chapter.

Based on international regulatory frameworks, African regulators need to have clear policy positions and regulations on a number of areas, namely:

- Data privacy, risk and security
- Data sovereignty
- Cybercrime
- Protection of intellectual property
- Vendor risk
- Migration complexity and operational risk

The financial regulators also need to work with other ministries in support of regional standards and harmonisation of rules that will ensure optimal portability of data for cloud services as well as allow CSPs to operate free from trade barriers. Regulators will also need to ensure ICT infrastructure, broadband deployment and connectivity are robust and data charges are affordable before financial institutions are allowed to adopt cloud banking. Building adequate ICT infrastructure that will provide affordable broadband access will require incentives for private sector investment in infrastructure as well as laws and policies that support universal access.

Data privacy, risk and security

Data privacy legislation is key to protecting the confidentiality of consumer and corporate data in the cloud.

As cloud solutions are typically delivered through physical servers which sit outside the financial service providers' own infrastructure (and may sit in other jurisdictions in the case for most African countries) and are owned and controlled by third-party CSPs, regulators need to define clear rules to minimise data security risks. Regulators will need to be specific on encryption and data access controls, how to ensure confidentiality and integrity of data, and how to prevent leakage of data.

In order to ensure data privacy and confidentiality, particularly in outsourcing data to third parties, African regulators need to uphold requirements that protect data subjects yet also allow CSPs to move data across borders freely and securely. Some of the key privacy and data protection requirements should require the consent of subjects for data processing, ensure the anonymity and privacy protection of collected data, provide data breach notifications, and safely handle the transfer of data across borders.

There are only 15 African countries that have fully implemented data protection legislation, leaving the majority of the continent with either no, or limited, data protection coverage. This leaves data subjects in these countries vulnerable to potential data security risks associated with cloud banking such as data leaks and cyberattacks.

Legislation should require financial institutions to evaluate the ability of the CSP to demonstrate its ability to restore and access personal data as well as implement appropriate controls, such as disaster recovery procedures.

Data-breach notifications are also an important control in data protection regulation. Currently, only three African countries require data-breach notifications. Financial sector regulation should require that data controllers notify regulators of personal data breaches within 72 hours of learning of breaches as well as provide specific details of the breach, such as the nature of the breach and the number of data subjects affected.

Financial institutions should also perform Data Protection Impact Assessments to identify any risks to consumer data that processing and data storage operations may present. The assessment should address the potential risk impacts, legal risks and compliance issues, and oversight limitations related to the countries where the outsourced services are to be provided and the data is to be stored. Regulators should also conduct regular compliance reviews of data protection policies to address any risks.

Confidential consumer data that is shared with third parties for processing should be auditable, where regulators have the right to review and audit financial institutions' outsourcing agreements with CSPs, as well as have full access to the CSPs' business premises for inspection purposes. Consumer permission as well as duration and contextual limits should determine the extent to which financial institutions share data with third-party CSPs. Consumers should also have the right to review and withdraw permissions to access their data at their discretion.

Regulators should ensure that financial institutions implement systems and processes that enable flexible data management to ensure that data is easily accessible and can be segregated so that consumers can move and review their data at any time. Financial institutions should communicate, in a simple and transparent manner, when persuading customers to share their data, as well as use encryption techniques to mitigate risk.

Regulatory requirements should also fall on the shoulders of CSPs, not just financial institutions. CSPs will need to develop and implement a number of internal practices to protect personal data against loss or exposure, as well as have full processing transparency. Regulators should hold financial institutions and CSPs responsible for non-adherence to these principles of regulation.

Data sovereignty

Regulators implement data sovereignty rules to protect jobs and grow domestic markets. However, in the case of technological innovation in Africa, the economies of scale are limited and data sovereignty legislation can increase the cost of providing financial services.

Data sovereignty rules negatively impact the ability to move data between countries. Even the largest CSPs and users do not maintain data centres in every jurisdiction in which they operate. In order for financial institutions to leverage cloud banking technology outside Africa, the cross-border movement of data needs to be unrestricted by the regulator.

African financial regulators will need to implement regulation that ensures there are no or few restrictions placed on cross-border transfers of data to allow CSPs to move data through the cloud in the most efficient way. Regulators will need to define the rules based on the quality of data protection legislation of the other country in which the CSP is based. If the other country's data protection legislation is strong, then the regulator should allow cross-border transfers of data to take place between financial institutions and CSPs.

Cybercrime

The large quantities of data that companies store in their computer networks are not only vulnerable to general data security risks, such as data leakage, but also cybercrime.

While countries like South Africa and Morocco have implemented specific national cybersecurity policy frameworks, the degree of protection against cybercrime varies across the continent. With only 15 African countries having adopted the AU Convention on Cybersecurity and Data Protection at various degrees, there is still space for improvement on the regulators' part to improve on security measures.

Regulators need to ensure that there are legislative, investigative and enforcement tools available to protect data subjects and data holders from cyber criminals. This involves creating and implementing cybercrime laws that protect data stored in the cloud from cyberattacks and unauthorised access. Furthermore, enforcing certification requirements on cybersecurity will ensure that financial institutions are well equipped to deal with cyberattacks.

Since cloud banking is conducted through internet connections, African regulators will need to enforce standards that ensure financial institutions have secure internet connections when transferring data to CSPs. Using firewalls will allow financial institutions to analyse incoming traffic on the network and assess which connections are unauthorised. Financial institutions and CSPs should also be required to heavily invest in security against viruses and malware.

Protection of intellectual property

CSPs rely on a combination of patents, copyrights and other forms of intellectual property protection to produce innovative cloud solutions. African regulators will need to ensure that there are strong intellectual property laws in place to protect cloud solutions from misappropriation and infringement of technology. Regulators should also incentivise CSPs to operate responsibly by not holding them to copyright liability when they do so.

African regulators will need to implement copyright laws that are consistent with international standards to protect CSPs and the laws will need to be effectively enforced and implemented. There should be detailed copyright protection for intermediaries, such as CSPs, where an internet intermediary cannot be held liable unless actual knowledge of infringement, or awareness of facts, or circumstances from which infringement is apparent exists. There also needs to be an active enforcement regime that will ensure the implementation of intellectual property legislation.

Vendor risk

Financial institutions that plan to use cloud services need to consider vendor risk. There are only a few major players in the market offering cloud services to financial institutions in Africa, i.e. Microsoft, Amazon and IBM. If one of these CSPs experience a major disruption in its services, there is a high probability that it will affect many financial institutions, and potentially the whole market.

African financial regulators will need to implement regulation on disaster recovery to ensure that financial institutions are protected in the scenario of system failures at the CSP. CSPs will need to have adequate controls in place to comply with laws on disaster recovery as well as service-level agreements in place that detail the responsibilities that CSPs have in lowering the risk of system outages and service disruptions.

Financial institutions will also need to take responsibility for potential risks that come with using CSPs and ensure that vendors maintain consistent compliance with regulation and internal policies. In order to understand and mitigate vendor risks, financial institutions should conduct vendor due diligence and continuous monitoring. African regulators will need to hold financial institutions accountable to having a strong vendor risk management programme where inherent risks are anticipated before adverse situations occur.

Migration complexity and operational risk

African regulators will need to monitor financial institutions' operational resilience in the wake of a disruption of cloud services. Financial institutions must be able to ensure continuity of service to customers by transitioning back to their own databases in the event of operational failures of CSPs, or if the services deteriorate to an unacceptable degree. International regulators have required that financial institutions have contingency plans and exit strategies in place in case of operational disruptions at CSPs.

African financial regulators need to adopt a supervisory approach that identifies where operational failures could have a significant impact on the economy and consider the levels of resilience they would expect financial institutions to demonstrate. Financial institutions should be required to implement policies that include contingency planning and a clearly defined exit strategy. Financial institutions should also ensure that they are able to exit cloud outsourcing arrangements if needed without undue disruption of their services to their clients, or adverse effects on their compliance with the regulatory regime.

Part 5

CONCLUSION

CONCLUSION

This report has highlighted the benefits that FSPs can gain from moving some or all of their operations to the cloud. Cloud banking can substantially reduce operating costs for FSPs of all shapes and sizes - changing large upfront investments to subscription fees, reducing training, configuration and system administration costs, while reducing the costs of maintaining traditional on-premise systems. New digital banks, like South Africa's TymeBank, have already demonstrated that, where regulations allow, they are able to make a massive (56%) cost saving by using cloud services. In competitive markets FSPs should pass these cost savings of using cloud to their current customers and, by providing more affordable products, expand their reach to the financially underserved and excluded.

African FSPs will also benefit from the flexibility of cloud operating models. Such models will allow FSPs to experience shorter development cycles for new products, and support faster and more efficient responses to customers' needs. Cloud technology will also allow small banks to adapt to digital change quickly and allow them to keep up with larger competitors in the market, including MNOs.

However, before FSPs can fully realise the benefits of the cloud they need to be sure that the telecommunications infrastructure is fit for their purpose and receives the support and blessing of the financial sector regulator. This report has provided a taxonomy of the issues involved in cloud banking from the perspective both of an FSP and a regulator.

Telecommunications infrastructure: In order to fully reap the benefits of cloud banking there needs to be extensive, stable and affordable broadband access. The majority of network infrastructure in Africa is below international standards. Fixed broadband connectivity varies across countries. Slow connectivity will inhibit African banks from fully benefiting from cloud technologies.

African telecommunications regulators will need to provide the spectrum and implement policies that incentivise investment to create developed broadband network infrastructure.

Regulatory reform: Many African banks are hesitant to adopt cloud banking because of the lack of clearly defined regulatory frameworks on cloud banking. Before banks can invest in cloud technologies, they need reassurance from the financial regulators that cloud usage will be permitted.

African financial regulators have a lot of work to do with regard to defining clear regulatory frameworks on cloud banking. Regulators will need to have detailed policy positions on data security and privacy, data sovereignty, cybercrime, intellectual property rights, vendor risk mitigation, and operational risk mitigation specific to cloud. A large amount of effort will need to go into defining policies and regulations around cloud and its usage in the financial sector, and in training regulators on the issue.

A clear and joined-up regulatory response is necessary to respond to the risk that the infusion of technology and finance creates while encouraging the significant opportunities for improved efficiency and costs, and better coverage of underserved consumers. It is incumbent upon regulators to take a balanced view and craft regulation and supervision in a way that ensures risks are appropriately mitigated, while not creating barriers to responsible innovation that improves access to financial services, customer experience and efficiencies within the financial system.

We would like to thank all contributors of this report as well as the leaders who are working to make the financial sector in Africa accessible for all Africans.

"With digitalisation come the opportunities to leapfrog development. Digital technology lowers costs and enhances efficiency while safeguarding inclusion" *Vera Songwe, Executive Secretary of the United Nations Economic Commission for Africa.*

G:ENESIS UNLOCKING VALUE

orange™ Business Services