MONOCLE

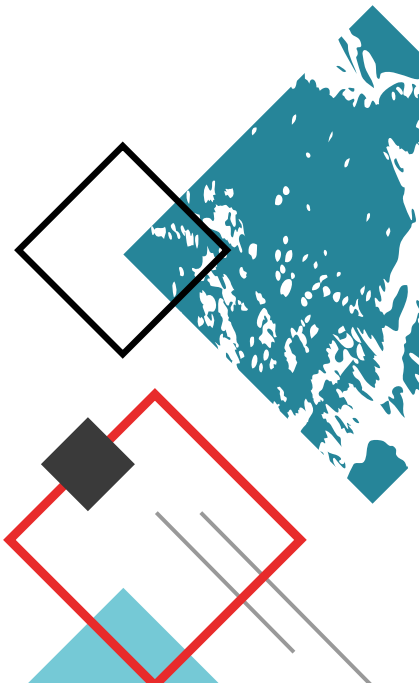
CLOUD REGULATION IN SOUTH AFRICA

Monocle Research Team

2020

MONOCLE

CONTENTS



MONOCLE

INTRODUCTION

Financial services companies are increasingly considering outsourcing to the cloud, as the benefits of this technology increase, and the risks diminish. Outsourcing in general is not new to firms and has been subject to requirements from regulators for over a decade. However, new technologies such as cloud computing and offshore data storage are changing firms' and regulators' relationship with outsourcing as they relate to these new technologies.

Regulators have traditionally taken a "technology neutral" approach to their regulatory positions, viewing the form of technology used as irrelevant to regulatory objectives. However, rapid adoption of cloud computing and data outsourcing among financial services companies has prompted regulators to depart from this neutral stance. This departure stems mainly from regulatory concerns around operational risk, security, risk concentration, and jurisdiction that pertain uniquely to cloud outsourcing.

Interest in cloud solutions is growing, with the benefits of this technology becoming increasingly accessible through improving security sytems and cost efficiencies, as well as operational benefits such as rapid scalability. Firms have been hesitant to transition to the cloud, partly because of the risks involved in a new technology, but also due to a lack of regulatory clarity and uncertainty over authority. More recently, however, regulators have attempted to address these shortcomings by releasing documentation clarifying their views on cloud outsourcing.

This paper provides an overview of the international regulatory landscape relating to cloud computing and data outsourcing in the financial services industry with a comparative focus on South Africa. It explains the approach taken by the Prudential Authority (PA) of the South African Reserve Bank (SARB) towards cloud and data offshoring and compares the South African approach to those of the United Kingdom, European Union, United States, Australia, and the Netherlands. The key regulatory issues and lessons for South African firms are also discussed.

WHAT IS CLOUD COMPUTING?

Cloud computing provides users with access to on-demand, **shared and configurable computing resources** hosted by third parties on the internet, instead of hosting their own on-premises IT infrastructure.[1]

The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[2]

According to NIST, cloud computing has five essential characteristics, three service models, and four deployment models.[3]

Essential characteristics:

i) **On-demand self-service**. Users of cloud services can unilaterally provision computing capabilities as needed without having to interact with the service provider.

ii) **Broad network access**. Cloud capabilities are accessible over the network through standard and heterogeneous platforms (for example, laptops or phones).

iii) **Resource pooling**. Cloud service providers pool their resources to serve multiple customers in a multi-tenant model, which helps reduce costs and ease scalability.

iv) **Rapid elasticity**. Providers can rapidly and elastically scale outward or inward according to demand.

v) **Measured service**. Cloud services automatically control, optimise, and report resource use, offering transparency to both customer and provider.

Service models:

Cloud computing has developed along three models, which vary in their complexity, degree of integration between firm and provider, and regulatory scrutiny.

i) **Infrastructure as a Service (IaaS)**. The customer is provided with processing, storage, networks, and other fundamental computing resources. The customer does not manage the underlying cloud infrastructure but retains control over operating systems, storage, applications, and possibly some network components.

ii) **Platform as a Service (PaaS)**. The provider deploys onto the cloud infrastructure the required applications. It is a platform for creating software that is delivered online. The customer has control only over which applications are deployed onto the infrastructure, but not over underlying infrastructure network, systems, and storage.

iii) **Software as a Service (SaaS)**. The provider provides users with its own applications on its own cloud infrastructure. The full end-to-end service is provided. The customer has no control other than some user-specific application settings. SaaS generally refers to end-user applications, such as Microsoft Office 365.

1. European Insurance and Occupational Pensions Authority (EIOPA), 2019
2. National Institute of Standards and Technology, 2011
3. NIST, 2011

Deployment models:

These cloud services are generally deployed through four models.[4]

i) **Private cloud services**. Cloud services are provided for exclusive use by a single organisation, comprising multiple business units.

ii) **Community cloud**. Cloud services are provided for exclusive use by a community of consumers with shared concerns, including several institutions of a single group.

iii) **Public cloud services**. Cloud services are provisioned for open use by the general public. The cloud infrastructure exists on the premises of the provider. Public cloud services could be free or on a pay-per-usage model.

iv) **Hybrid cloud services**. The cloud infrastructure is composed of two or more distinct cloud infrastructures that remain unique entities but are joined by technology, allowing portability.

WHAT ARE THE BENEFITS OF THE CLOUD?

Financial services companies must weigh up the costs and benefits of outsourcing cloud-based services to the cloud compared to existing data centres. Most firms have invested heavily in on-premises data infrastructure that was built fit-for-purpose based on the requirements and technologies at a specific time. Much of this legacy infrastructure is outdated and poses great financial and operational risks to the organisation. The main problems with legacy data infrastructure are complexity, security, and cost.

> **The European Insurance and Occupational Pensions Authority (EIOPA) views the benefits of moving to the cloud in five areas: scale, resiliency, privacy, security, cost and time to the market.**

Outsourcing to the cloud mitigates the problems associated with existing on-premise data centres, but also comes with risks of its own. The European Insurance and Occupational Pensions Authority (EIOPA) views the benefits of moving to the cloud in five areas: **scale**, **resiliency**, **privacy**, **security**, **cost** and **time to the market**.[5]

Scale

The cloud benefits from essentially unlimited capacity. This capacity is also flexible, allowing customers to scale up or down as needed. This avoids the problem of overprovisioning, which is cost inefficient, and under-provisioning, which would shut down operations.

Resiliency

Cloud applications are built to be permanently online and resilient to disruptions if any parts of the system fail. This is achieved through auto-scaling, load balancing, backups, copying to multiple locations, and other methods.

4. EIOPA, 2019
5. EIOPA, 2019

Privacy

Sensitive data is protected through the privacy design features of cloud infrastructure. Internal walls ensure different areas are separated and can be accessed only by authorised individuals or groups within the customer institution. Cloud service providers have data centres in numerous geographic locations to address different regulatory requirements.

Security

Cloud service providers have built their infrastructures to meet the strictest security requirements at every level. While security threats do still exist, the cloud has become more secure than most outdated on-premise infrastructure.

Cost & Time to Market

The cloud will cost less for most configurations, due to its scale, resource sharing, automation, standardisation, and other advantages. These also allow for faster time to market, experimentation, and immediate results. There is also less need for maintenance. Cloud customers can more easily scale operations to larger regions at lower costs than under traditional IT models.

Overall, the benefits of using the cloud are clear and growing. The cloud has changed the way financial services companies consume technology, **moving away from the consumption of IT products to the consumption of IT services on a needs basis**.

These benefits are especially effective for new entrants building directly onto the cloud from the outset. Incumbent firms migrating from old infrastructure face greater costs and complexity and it will take longer for them to experience the same benefits.

WHO ARE THE SERVICE PROVIDERS?

The cloud market is dominated by several companies that have seized the economies of scale and network economies offered in the cloud computing industry. The market shares of these companies differ depending on the service model – some are more established at SaaS whilst others focus on PaaS. Because financial services firms will be outsourcing different business areas to different models and even different companies, it is worth looking at how CSPs compare at a service model level.

SaaS is the most established cloud service model and is still growing healthily. The SaaS market is dominated by five key companies which account for just over half of SaaS market share globally. **Microsoft** leads the way with 17% of the market and impressive growth of 34%. It is followed by **Salesforce** and **Adobe** with market shares of 12% and 10% respectively. **SAP** and **Oracle** each have a 6% market share. The rest of the market is occupied by 10 other companies, including Google and IBM.[6]

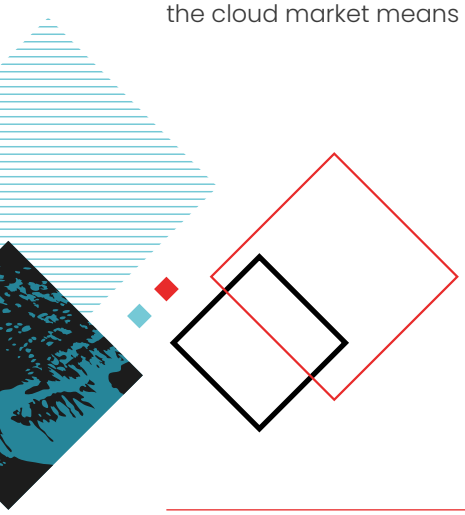
The IaaS market is the most concentrated of the models. It is dominated by five companies who hold close to 80% of market share. These vendors are **Amazon** (47.8%), **Microsoft** (15.5%), **Alibaba** (7.7%), **Google** (4.0%) and **IBM** (1.8%).[7]

6. Jones, 2020
7. Jones, 2020

Unlike SaaS and IaaS, the PaaS market is much more difficult to dominate. According to a study by Gartner, only 10 of 360 existing vendors were able to provide more than 10 of 22 PaaS service categories.[8] Unsurprisingly, the 10 include the biggest cloud companies such as **Microsoft**, **Amazon**, **Google**, etc.

While almost all the largest cloud service companies are based in the United States, their data centres could be located anywhere in the world. This means that a firm outsourcing its data to the cloud of an American vendor could actually be storing its data in India, for example. This raises questions around jurisdiction that many regulators have sought to clarify. Fortunately, South Africa hosts the data centres of several large players. This lessens jurisdictional issues in South Africa, and may potentially make cloud migration even more cost effective.

In sum, the cloud market is dominated by a few major vendors. South African financial services firms will almost certainly continue to outsource their cloud computing needs to these companies. The nature of the cloud market means concentration risk and jurisdictional issues are important regulatory concerns.



WHAT ARE THE KEY REGULATORY CONCERNS AROUND CLOUD COMPUTING?

The primary focus of regulators when it comes to cloud outsourcing is operational resilience. This is evident in the emphasis placed on risk assessment, due diligence, good governance and accountability in regulators' proposals. Regulators expect firms to have a robust business case for moving to the cloud, a deep understanding of the risks involved, and a risk management framework in place that can mitigate against these threats.

Migration to the cloud comes with significant operational risk, as incumbent institutions must execute migration with proper preparation, governance, and control, whereas new entrants are able to build straight from the cloud. A Financial Conduct Authority (FCA) survey found that failed IT transitions were the cause of one-fifth of all operational incidents reported between October 2017 and September 2018.[9] Ensuring firms follow best practice to improve operational resilience is a regulatory priority.

Another challenge to operational resilience is the "**shared responsibility model**" inherent in outsourcing to a cloud service provider. In this model, the firm outsourcing to the cloud remains responsible for the data, even if the cloud service provider is the de facto owner of the data. It is difficult for the senior managers and heads of IT and data areas in a firm to achieve full and transparent oversight of the provider and its controls and security measures. Yet were something to go wrong, these managers would be held responsible in the eyes of regulators. This dynamic explains the focus regulators have placed on ensuring firms implement proper risk and data management frameworks and maintain clear contractual documentation of outsourcing arrangements. Crucially, this accountability approach means cloud users have an incentive to follow the advice of regulators when entering cloud outsourcing arrangements.

8. Gartner, 2019
9. FCA, 2018

Security risk is related to the operational risk of cloud outsourcing. Financial institutions deal with highly sensitive transactional and customer data. If a breach takes place and data is lost or duplicated, the financial institution will face severe reputational consequences, regardless of whether the cloud service provider was at fault. This could put the institution's continuity at risk. Regulators therefore urge firms to ensure that their cloud vendors meet security standards.

A second major concern for regulators relates to **jurisdiction**. Occasionally, the server that hosts a company's data will not be in the same jurisdiction as the company itself. Regulators may be limited in their jurisdiction over data that has been offshored to a foreign country. The unification of cloud regulation around the world will mitigate this concern.

Another concern surrounding cloud outsourcing is concentration risk. A handful of cloud service providers control most of the market, which means there is significant concentration risk. Regulators are rightly concerned about this, due to the highly sensitive nature of banking data. If a cloud vendor were to fall victim to a debilitating cyber-attack, this single point of failure could expose the sensitive data of several firms.

> **"A handful of cloud service providers control most of the market, which means there is significant concentration risk."**

Additionally, moving from one CSP to another is a massively costly and time-consuming exercise, meaning firms are essentially "locked-in" once they commit to outsourcing to a provider. Many regulators, including those in South Africa, have therefore included the need for "**exit plans**" and **contingency arrangements** when entering into outsourcing arrangements.

WHAT IS THE REGULATORY STANCE ON CLOUD OUTSOURCING IN SOUTH AFRICA?

The Prudential Authority (PA) of the South African Reserve Bank (SARB), recognising the increasing interest in the cloud, clarified its position in September 2018, when it issued a **Directive (D3/2018)**[10] and **Guidance Note (G5/2018)**[11] on "Cloud Computing and Data Offshoring by Banks". The directive is applicable to "all banks, controlling companies, branches of foreign institutions and auditors of banks or controlling companies". The directive became effective from 1 October 2018.

The directive sets the PA's requirements for cloud computing and data offshoring. It is intended to be read in conjunction with the guidance note, which is provided to assist banks to comply with and better understand the requirements in the directive.

The PA directive is **principles-based**, allowing banks some room to decide how to approach their adoption of cloud computing and data offshoring. The PA expects banks to follow a **risk-based approach** that is in line with their risk appetite, based on the nature and size of their operations, when transitioning to the cloud. Instead of being prescriptive and strict in its position, the PA places the responsibility under the ambit of banks' corporate governance processes.

10. PA, 2018a
11. PA, 2018b

As part of sound corporate governance relating to cloud computing and data offshoring, banks must have in place a formally defined and board approved data strategy and data governance framework. According to the guidance note, the data strategy should include:

a) How a bank classifies its data
b) Where (in which jurisdictions) data may be stored
c) Which service and deployment models of cloud storage are applicable to which classifications of data
d) Which security requirements and restrictions are applicable to the different classifications of data
e) The process in the case of data loss and/or breach.

More specifically, banks pursuing cloud data storage or offshoring of data must have a clearly defined policy for such activities, aligned with risk strategies and data governance frameworks. Additionally, oversight of these activities must be incorporated into corporate governance structures. As well as assessing whether undertaking cloud computing or data offshoring is within a bank's risk appetite, it should follow appropriate due diligence.

Security is a major concern surrounding all data storage, especially with the relatively new and untested cloud data storage. The PA thus directs banks to take "all reasonable measures" to preserve the confidentiality and integrity of their data. This is an example of the relatively vague nature of the PA directive: it does not define what is considered "reasonable", leaving the interpretation of its rules to the banks.

The issues surrounding jurisdiction become more complicated when moving from on-premises data storage to cloud data storage and offshoring. The PA directive touches on this issue, requiring banks to ensure they are compliant with legislation and regulations both locally and in the country in which cloud services and/or data are hosted. As mentioned, South Africa hosts several data centres anyway. Additionally, the transition to the cloud should not impede in any way the regulators' ability to fulfil their duties.

"As part of sound corporate governance relating to cloud computing and data offshoring, banks must have in place a formally defined and board approved data strategy and data governance framework."

The directive does not call for any new reporting requirements, over and above existing requirements. Banks are directed to provide the PA with information relating to material cloud computing and data offshoring arrangements, but this was already a requirement under Guidance Note 5/2014. In this case, cloud outsourcing is not treated differently from general outsourcing from a reporting perspective.

Lastly, the PA requires banks to consider the directive in the context of their other legislative obligations to the Financial Intelligence Centre (FIC) and the Financial Surveillance Department, which may have different statutory objectives and requirements. At the time of writing, neither of these institutions had issued guidelines relating specifically to cloud data storage over and above existing data security requirements.

WHAT ARE THE REGULATORY POSITIONS ON CLOUD OUTSOURCING IN OTHER COUNTRIES?

It is advisable for South African financial services companies to familiarise themselves with cloud regulations in other countries, as these may indicate trends and emerging best practices that could be emulated by the South African regulator. Keeping up to date could reduce the costs of implementing new regulation later, as well as strengthen governance and reduce risk exposure to the cloud. This section covers cloud regulation in the United Kingdom, United States, Europe, the Netherlands, and Australia.

United Kingdom: Financial Conduct Authority

The Financial Conduct Authority (FCA) of the UK published guidance for firms outsourcing to the cloud and other third-party IT services.[12] The final Guidance (FG16/5) was published in July 2016. As part of the FCA's mandate of consumer protection, guidance FG16/5 applies to all relevant firms and not just banks and other financial services.

The FCA guidance is similar to the guidance released by SARB. Its purpose is to clarify the requirements for firms moving to the cloud. The considerations within the guidance take a similar principles-based approach that leaves space for firms to outsource to the cloud, subject to their own internal risk-based policies.

Before outsourcing to the cloud, in the view of the FCA, a firm should have a clear business case to do so, in line with its risk appetite and data policies, after observing due diligence. As part of the due diligence exercise, firms should ensure that their operational risk is not worsened by entering into an outsourcing agreement. As part of firms' risk management, they should assess whether the regulatory risks differ if those involved in providing or using the cloud service are in different jurisdictions. Firms are also required to perform a security risk assessment. Notably, the FCA asks firms to monitor concentration risk and consider the implications if a cloud service provider were to fail.

The guidance calls on firms to follow international best practice and ensure the cloud service provider meets international standards. Notably, the guidance states that "firms retain full accountability for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider". [13]

The FCA communicated its intent to comply with European Banking Authority (EBA) guidelines on outsourcing recommendations, which were published in February 2019. The FCA guidance (FG16/5) still applies to all firms under its authorisation, but the EBA guidelines also apply to credit institutions and investment firms.

12. FCA, 2019
13. FCA, 2019

UK: Prudential Regulation Authority

The Prudential Regulation Authority (PRA) published Consultation Paper 30/19 on "Outsourcing and Third-party Risk Management'.[14] While this is merely a consultation paper, and therefore does not place requirements on firms beyond those discussed above, it represents the best view of the road ahead for cloud regulation (at least in the UK).

The paper, published on 5 December 2019, seeks to modernise the regulatory framework on outsourcing, facilitate greater adoption of the cloud, and implement the EBA guidelines. It is relevant to all UK banks and investment firms, insurance and reinsurance firms, and branches of overseas banks and insurers.

Overall, the PRA paper complements the EBA guidelines. It is intended to harmonise the approach of UK firms with those in Europe. The key departure from the FCA regulation, therefore, is the requirement for an outsourcing register, which was first mentioned in the EBA guidance note.

Europe: European Banking Authority

The EBA finalised its report on outsourcing recommendations, including those relating to the cloud, in February 2019. The guidelines set out specific provisions for the governance frameworks of financial institutions regarding their outsourcing arrangements and related supervisory expectations and processes. The guidelines seek to clarify regulatory expectations, including documentation, risk assessment, and governance and controls around outsourcing. The recommendation on outsourcing to cloud service providers, published in December 2017, has been integrated into the guidelines.

Operational risk is a key area of concern for the EBA, consistent with other authorities. The confidentiality, integrity, and availability of data and related systems require protection as these pose serious operational risks to firms. Concentration risk is another key concern, especially relevant to cloud and other IT outsourcing. The EBA also expresses the need to monitor and manage concentration risk.

The EBA, like the SARB, places responsibility on firms to define data security requirements and to monitor service provider compliance on an ongoing basis. As part of the risk-based approach, firms should consider the risks involved in chosen data storage and processing locations and information security considerations.

An important aspect of the EBA outsourcing guidelines is its documentation requirements. The guidelines state that banks should maintain an updated register of information on all outsourcing arrangements. This 'outsourcing register' should include all past and existing outsourcing arrangements, as well as distinguish between crucial or important outsources functions. The EBA guidelines include several other detailed requirements for the register. This requirement is essentially the same as that required in South Africa, where banks are required to report material outsourcing arrangements, as per Guidance Note 5/2014. On the other hand, the EBA's concern about concentration risk is absent from any regulatory framework in South Africa.

The EBA ultimately expects regulators to assess firms' outsourcing plans on a case-by-case basis. Authorities are expected to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring risk concentrations and assessing whether or not such concentrations pose a threat to the stability of the financial system. Firms should provide authorities with comprehensive documentation on outsourcing arrangements.

14. PRA, 2019

The EBA is directed only at banks and investment institutions. In the insurance sector, the European Insurance and Occupation Pensions Authority (EIOPA) recently issued a consultation on guidelines to cloud outsourcing, which is intended to come into force in January 2021. The EIOPA guidelines were released in order to avoid regulatory fragmentation after the EBA published its guidelines. Recognising that the risks posed by cloud outsourcing are similar across sectors, the EIOPA guidelines are almost identical to those of the EBA.

Australia: Australian Prudential Regulation Authority

The Australian Prudential Regulation Authority (APRA) released an information paper entitled "Outsourcing involving cloud computing services" in July 2015.[15] This paper clarified regulation around cloud computing usage by banks, insurance companies, and retirement funds as a response to the increase in interest in cloud computing.

It emphasised that good corporate governance was required by financial institutions for adoption of the cloud. This entails the board evaluating the level of risk that migrating would result in and ensuring that it is in line with the risk appetite of the company; the due diligence that is required when choosing a provider; ensuring data protection and security for the data stored on the cloud; change management; and the transitioning process of migrating.

In 2018, APRA updated this information paper. The updated paper acknowledged the improvement of security risk by cloud vendors since 2015 but still cautioned how financial companies approach the risk that is inherent in cloud computing. The paper identifies that arrangements with different levels of risk should be treated differently. The nature of usage was divided into three categories: low inherent risk, heightened risk, and extremely heightened risk.

Low inherent risk involves cloud computing with no offshoring and the regulator does not expect financial institutions to consult with them before entering into this agreement; however, they do expect to be notified within 20 days of the agreement being finalised. Heightened risk projects, which include offshoring agreements, are expected to be consulted on with APRA once the internal governance process of the financial institutions is completed. For those that are extremely heightened risk, institutions need to consult with APRA from a very early stage of the process, once a proposal has been drawn up and initial approval has been granted. Extreme inherent risk is regarded as anything that could result in the threat of business continuity if the system is breached.

APRA's method of classifying projects according to risk is unique among the regulators covered in this paper. Another unique aspect is the clause on when to consult and when to notify the regulator. This could be an indication of future approaches to be adopted by other regulators such as South Africa's.

15. APRA, 2018

United States: Federal Financial Institutions Examination Council

The US has several banking regulators, which can cause confusion as to which regulator is the primary authority. The Federal Financial Institutions Examination Council (FFIEC) is a group of regulators which includes five banking regulators: the Federal Reserve Board of Governors, the National Credit Union Administration, Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. The grouping of these regulators enables a more uniform set of regulation.

The FFIEC IT Subcommittee released a statement in July 2012 entitled "Outsourced Cloud Computing".[16] The FFIEC recognised cloud computing as another form of outsourcing with similar risks and therefore encouraged financial institutions to refer to their earlier outsourcing guidance. This statement brings to light risks that affect cloud computing that already exist in the previous guidance. The regulator highlights the importance of due diligence when a provider is chosen and financial institutions are advised to consider factors such as whether the provider will cost the company a fee that is on budget and more importantly whether they are compliant with regulatory requirements.

The statement identifies data classification, segregation, and recoverability as areas financial institutions should address, but the regulator does not go into detail as to how, for example, different data classes should be treated. They also recommend that financial institutions ensure that data can be removed from all server locations where it is stored before entering into an agreement as this may pose a risk when the contract ends. They should also consider whether the provider can ensure business continuity in case of an unexpected disruption. In 2018, the US National Treasury released a report on cloud computing whereby they advised the FFIEC to modernise their regulation on cloud computing to provide clarity to financial institutions.

Netherlands: De Nederlandsche Bank

The Central Bank of Netherlands (De Nederlandsche Bank; DNB) is the prudential supervisor of financial organisations in the Netherlands. It works hand in hand with the EBA and therefore, all financial institutions supervised by the DNB must also comply with EBA policy. The DNB also views cloud computing as a form of outsourcing and therefore, financial institutions that enter cloud agreements should be compliant with all outsourcing regulation.

The Circulaire Cloud Computing was published by the DNB in 2012.[17] It expects financial institutions to submit a risk analysis template provided by the regulator. This risk analysis covers topics such as compliance with current regulation, reliability of service provider, location of servers, data confidentiality, integrity and availability. The Dutch regulator also requires that the cloud arrangement does not in any way obstruct their supervision. An agreement between the service provider and financial institution needs to be drawn up that navigates the possibility of supervision directly or by proxy on the premises of the third party.

See page 15 for a table summary on how the regulators

16. FFIEC, 2012
17. DNB, 2012

STRENGTHS AND WEAKNESSES OF SARB CLOUD REGULATION

The previous section shows that the South African approach to cloud outsourcing is largely the same as authorities in other jurisdictions. While some regulators have more stringent reporting requirements and other regulators suffer from less clarity and depth in their views, there is alignment in their principles-based approaches. Nevertheless, South Africa's regulatory approach to cloud outsourcing has some strengths and weaknesses.

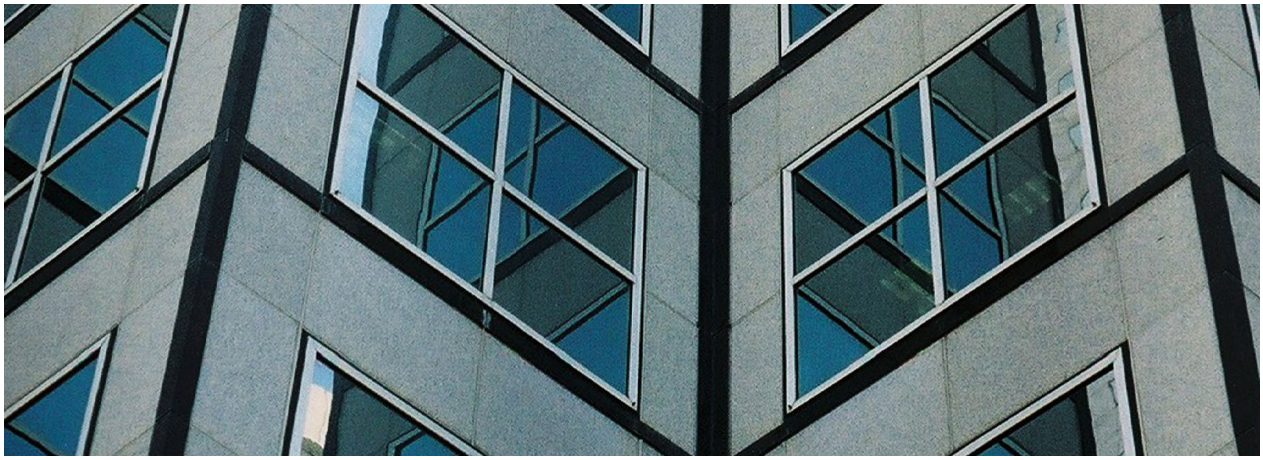
The most obvious strength of South African regulation is that there is no confusion around which institution is the chief authority on cloud regulation for banks. The PA has made it clear that it is the body in charge of setting regulations for banks in relation to cloud computing and data offshoring. While the PA directive does remind banks to consider their obligations to other regulators, such as the FIC, the PA is the leading body on this topic.

The second (potential) strength is the fact that the PA has not been overly restrictive and prescriptive in its approach to cloud regulation. As discussed, the PA directive and guidance note leave sufficient freedom for banks to adopt the cloud, subject to their internal processes.

On the other hand, this lack of specificity could be a weakness, if it means banks remain hesitant to move over to the cloud, as long as they believe regulators could harden their stance, making compliance a greater burden in the future.

Another weakness is that, despite clarity in relation to banks, insurance companies have not benefitted from similar communication and clarification of requirements in relation to the cloud. Although the PA regulates banks and insurers according to The Financial Sector Regulation Act (2017), the cloud computing guidance only listed banks, controlling companies and foreign branches as the targeted institutions. Seeing as insurers have similar incentives to move to the cloud, regulators should step in to clarify whether their stance is the same for insurance companies as it is for banks.

One area in which a foreign regulator is more stringent or more specific than in South Africa is the risk levels approach adopted by APRA. This is an interesting, more focused approach that could strengthen the SARB's position on the cloud.



KEY CONSIDERATIONS FOR SOUTH AFRICAN INSTITUTIONS CONSIDERING CLOUD OUTSOURCING

While there is still ample space for the further development of the regulatory framework governing movement into the cloud, the PA expects banks to:

- have a solid business case for moving to the cloud.
- assess the risks of offshoring to the cloud (to the bank, customers, and the wider system).
- develop sufficient capabilities to manage these risks.

Banks should focus on improving their internal understanding of the costs and benefits of adopting the cloud and increasing technical capacity in relation to the cloud. Even though it will be outsourced, it is crucial to have capable personnel within the bank that are able to monitor outsourcing arrangements, and to ensure they are compliant, within the risk profile, and sufficiently documented. This is the best way to ensure operational resilience under the 'shared responsibility' model inherent in cloud outsourcing arrangements.

Banks and insurers moving to the cloud must go above and beyond regulatory requirements, following the best regulatory practices from around the world and the best internal data governance policies. They must ensure that there is a clear understanding of the data, processes, systems, ownership, intended use and allowed use in order to meet data requirements.

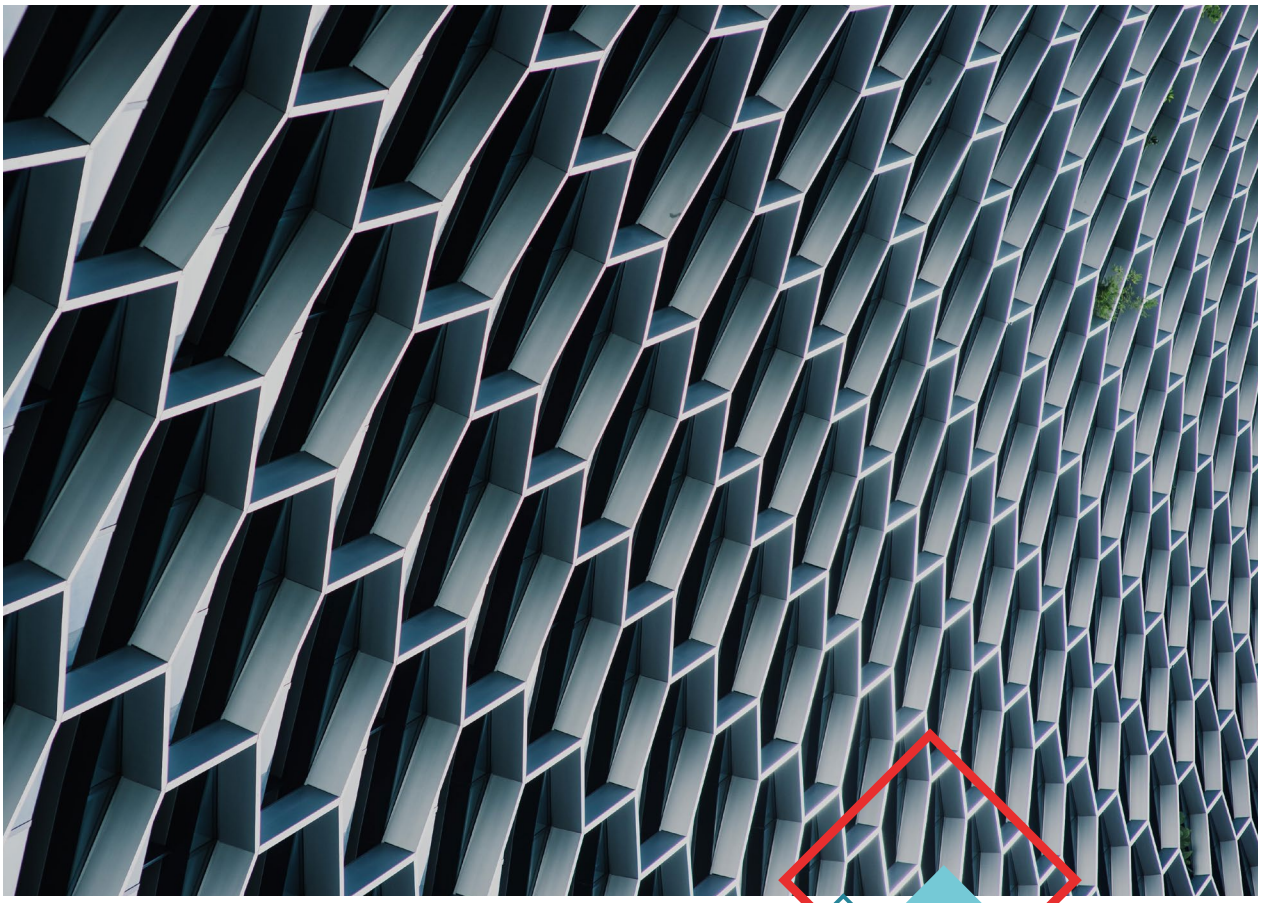
Banks are currently on a mission to leverage data as an asset and manage data more effectively as required by BCBS 239. Monocle can assist our clients by ensuring that the data architecture and landscape is clearly understood such that governance policies are adequality designed and implemented, according to the latest regulatory requirements, including those prescribed by the BCBS.

CONCLUSION

Cloud technology is no longer the future, it is the present. As the benefits of migrating to the cloud increase, more and more companies will outsource their data storage to cloud service providers. Regulators have realised the need to clarify their stance on cloud computing and outsourcing, in order to avoid unnecessary complexity caused by regulatory uncertainty.

In South Africa, the PA at the SARB is one of many regulators that has issued documentation with the intention of clearing up cloud outsourcing policy. This paper has discussed the South African regulatory approach, finding that it is not overly restrictive or burdensome. Other countries, such as Australia, have more stringent reporting and oversight requirements, and this may indicate that South African regulations may tend to become more prescriptive in the future. Some suffer from greater uncertainty than in South Africa due to a lack of a unified regulatory stance, such as the United States.

Overall, regulators generally adopt a principles-based approach to cloud outsourcing, largely following existing regulation on outsourcing and offshoring. Banks and insurers that are considering a transition to the cloud must have in place sound corporate governance and data policies, ideally with a focused cloud strategy. Firms should ensure there is a solid business case, considering the risks involved, and develop effective internal capabilities to manage the unique risks involved in cloud outsourcing.



ABOUT MONOCLE

Monocle is an independent, results-focused management consulting firm specialising in banking and insurance with almost two decades of experience working alongside industry leading banks and insurance companies around the world. With offices in London, Cape Town and Johannesburg we service our clients across the United Kingdom, Europe, Scandinavia, Asia, South Africa and much of Sub – Saharan Africa.

We design and execute bespoke change projects, from start to finish, bridging the divide between business stakeholders' needs and the complex systems, processes and data that sit under the hood. We offer several unique capabilities to our clients, which have been forged over time through the combination of a highly specialised skillset and extensive experience working with the systems, processes and people that are at the heart of the financial services industry.

SUMMARY TABLE: HOW DO REGULATORS COMPARE?

	USA	EU	UK	AUS	NED	SA
Authority	FFIEC	EBA	FCA & PRA	APRA	DNB	SARB
Principles Based?	Yes	Yes	Yes	Yes	Yes	Yes
Risk Approach	The FFIEC Statement recognises cloud computing as a form of outsourcing and therefore, advises companies to follow the outsourcing manual as their approach to risk. The statement further highlights risks that could be specific to cloud computing such as data classification, segregation and recoverability.	The EU highlights operational risk and concentration risk as key areas of concern. They urge monitoring these risks closely.	The FCA encourages risk analysis to ensure the given risk is in line to the company risk. They also warn of concentration risk and what the implications would be if a cloud service provider were to fail. The PRA takes a similar stance to the FCA only differing with outsourcing registers stipulated by the EBA.	The APRA regulation emphasises on financial institutions evaluating risk advising that risk should be approached differently at different risk levels.	The DNB takes a risk centred approach by requiring institutions to submit risk evaluations following a given risk analysis template. The template covers topics such as reliability of service provider, location of servers, data confidentiality, integrity and availability	The SARB puts the responsibility of assessing risk and ensuring it is aligned with the company's risk appetite on the company itself. It stipulates that banks should focus on classification of data, jurisdiction of where its stored and risk of data loss/breach.
Risk Level Classification	None	None	None	ARPA divides risk levels to low inherent risk, heightened risk and extremely heightened risk.	None	None
Consultation with regulator required	None	None	None	If a project's risk level is considered heightened, consultation is required after internal governance process is concluded. If the risk is considered to be extremely heightened, consultation is required after internal proposal is approved	None	None
Notifying the regulator requires	None	The EBA requires financial institutions to keep an updated register of all outsourcing arrangements, distinguishing between important functions that have been outsourced.	None	When projects have low inherited risk, APRA should be notified within 20 days of the cloud arrangement being concluded.	DNB requires to be notified before financial institutions enter into any cloud arrangement.	Banks are directed to provide the PA with information relating to material cloud computing and data offshoring arrangements
Applies to insurance	Yes	No, insurance companies need to follow the European Insurance and Occupation Pensions Authority (EIOPA) guidelines which will come into effect July 2020. This regulation is nearly identical to that of EBA.	Yes	Yes	Yes	No
Jurisdiction	All financial institutions and insurance companies governed by the 5 regulators in the USA.	All lending banks, investment firms, and credit institutions in countries that form part of the European Union.	All banks and insurers in the UK should comply with FCA. The FCA intends to be in line with EBA guidelines released in 2019. Investment banks and credit institutions need to also be in compliance with EBA. The PRA guideline will be relevant to banks, investment firms, insurance, reinsurance firms and branches of overseas banks and insurers. It complements the EBA guidelines.	All financial institutions, insurance companies and retirement funds in Australia.	DNB works hand-in-hand with the EBA. All financial institutions and insurers in the Netherlands need to be in compliance with both DNB and EBA. If uncertainty exists between the two regulators, comply with the EBA.	All South African banks, controlling companies and branches of foreign financial institutions need to comply with SARB PA guidelines.
Other regulations to comply with governing data protection.	The USA does not have a federal level data protection regulation for consumers.	GDPR	GDPR	The Australian Privacy Act	EBA	POPI
Guideline or Policy?	Guideline	Guideline	Guideline	Guideline	Guideline	Guideline

REFERENCES

FirstRand. 2019. Annual Report. Retrieved 19 April 2020, from https://www.firstrand.co.za/media/investors/annual-reporting/firstrand-annual-integrated-report-2019.pdf

Finastra. 2018. Banks in Singapore rank highest in Asia Pacific in Open Banking Readiness according to the Finastra Inaugural Open Banking Readiness Index. Retrieved 20 April 2020, from https://www.finastra.com/news-events/press-releases/banks-singapore-rank-highest-asia-pacific-open-banking-readiness
Circulaire Cloud Computing. 2012. Retrieved 19 April 2020, from https://www.toezicht.dnb.nl/en/binaries/51-224828.pdf

European Banking Authority. 2019. Final Report on EBA Guidelines on outsourcing arrangements. 25 February 2019. Available: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1 [April 7, 2020].

European Insurance and Occupational Pensions Authority. 2019. Outsourcing to the cloud: EIOPA's contribution to the EU Commission fintech action plan. 27 March 2019. Available: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_outsourcing_to_the_cloud_contribution_to_fintech_action_plan_3.pdf [April 23, 2020].

Financial Conduct Authority. 2018. Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018. November 2018. Available: https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf [April 16, 2020].

Financial Conduct Authority. 2019. Finalised Guidance FG 16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services. September 2019. Available: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf [April 7, 2020].

Gartner. 2019. Gartner Says Nearly 50 Percent of PaaS Offerings Are Now Cloud-Only. Gartner. 27 February 2019. Available: https://www.gartner.com/en/newsroom/press-releases/2019-02-27-gartner-says-nearly-50-percent-of-paas-offerings-are- [April 26, 2020].

Gartner. 2019. Gartner Forecasts IT Spending in South Africa Will Grow 3.9% in 2019. Retrieved 19 April 2020, from https://www.gartner.com/en/newsroom/press-releases/2019-07-24-gartner-forecasts-it-spending-in-south-africa-will-gr

Goasduff, L. 2019. Cloud Adoption: Where Does Your Country Rank? Retrieved 19 April 2020, from https://www.gartner.com/smarterwithgartner/cloud-adoption-where-does-your-country-rank/

How reliant are banks and insurers on cloud outsourcing? 2020. Retrieved 19 April 2020, from https://www.bankofengland.co.uk/bank-overground/2020/how-reliant-are-banks-and-insurers-on-cloud-outsourcing

Jones, E. 2020. Cloud Market Share – a Look at the Cloud Ecosystem in 2020. Kinsta. 10 April 2020. Available: https://kinsta.com/blog/cloud-market-share/ [April 27, 2020].

National Institute of Standards and Technology. 2011. The NIST Definition of Cloud Computing. Peter M. Mell and Timothy Grance. Available: https://www.nist.gov/publications/nist-definition-cloud-computing [April 25, 2020].

Outsourced Cloud Computing. 2012. Retrieved 19 April 2020, from https://ithandbook.ffiec.gov/

Outsourcing Involving Cloud Computing Services. 2020. Retrieved 19 April 2020, from https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf

Prudential Authority. 2018. Directive D3/2018. South African Reserve Bank. Available: https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/8749/D3%20of%202018.pdf [April 6, 2020].

Prudential Authority. 2018. Guidance Note G5/2018. South African Reserve Bank. Available: https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/8747/G5%20of%202018.pdf [April 6, 2020]
Prudential Regulation Authority. 2019. Consultation Paper CP30/19: Outsourcing and third party risk management. Bank of England. December 2019. Available: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultationpaper/2019/cp3019.pdf?la=en&hash=4766BFA4EA8C278BFBE77CADB37C8F34308C97D5 [April 7, 2020].

Raymond, K. 2018. More Than 70% of Insurers Use Cloud Computing - Novarica. Retrieved 19 April 2020, from https://novarica.com/2018/04/70-insurers-use-cloud-computing/

Reeves, A. 2019. Is a More Favourable Wind from Regulators Blowing Away Cloud Concerns Among Banks? Temenos. 4 July 2019. Available: https://www.temenos.com/news/2019/07/04/are-regulators-reducing-cloud-concerns/ [April 6, 2020].

JOHANNESBURG

13th Floor, Greenpark Corner,
3 Lower Road, Morningside,
Sandton, South Africa

Phone: +27 (0) 11 263 5800
Fax: +27 (0) 11 263 5811
Website: www.monocle.co.za

CAPE TOWN

301 New Cumberland,
163 Beach Road, Mouille Point,
Cape Town, South Africa

Phone: +27 (0) 82 952 1415
Website: www.monocle.co.za

UNITED KINGDOM

4 Lombard Street,
London,
EC3V 9HD, England

Phone: +44 (0) 2071 902 990
Website: www.monocle.co.uk

Cloud Regulation in South Africa

MONOCLE