BDO

BDO IN SOUTH AFRICA | FINANCIAL SERVICES

NAVIGATING THE CLOUD

AUDIT • ADVISORY • TAX

TABLE OF CONTENTS

AN INTRODUCTION TO CLOUD COMPUTING

Christopher O'Flaherty, Scott Hewitt, Reshelle Naidoo
BDO Financial Services Team

The internet is synonymous with the Cloud. At the consumer level, it usually refers to photo, video or document storage (like iCloud, OneDrive or Dropbox), that can be accessed from anywhere. But Cloud computing refers to anything that involves delivering services over the internet, as opposed to software or hardware installations on individual devices.

Cloud computing can also be thought of as utility computing, or on-demand computing.

The name Cloud computing was inspired by the cloud symbol that is often used to represent the internet in flowcharts and diagrams.

Cloud computing is one of the hottest sectors in the business-technology market. But the window of opportunity for companies to grab a piece of it, is closing fast. Leveraging new emerging technologies like Cloud computing can drive organisations to increase revenue, cut costs, and improve overall operations.

Organisations of every industry are using the Cloud for a wide variety of use cases, such as data backup, disaster recovery, email, software development and testing, big data analytics, and customer-facing web applications. An example in our industry of financial services includes the use of the Cloud to power real-time fraud detection and prevention but more on this later.

Cloud computing is the on-demand delivery of computing power, database storage, applications and other IT resources through a Cloud services platform via the Internet which often features pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centres and servers, you can access technology services on an as-needed basis from a Cloud provider such as Amazon Web Services (AWS) or Google Cloud Platform (GCP).

ADVANTAGES OF CLOUD COMPUTING

In the end, all Cloud services share the same end goal: To provide easy, scalable access to resources and IT services. Some specific benefits include:

- **Self-service provisioning:**
  Users have access to any type of compute resources for their workloads on demand. A user can provision their server time and network storage, removing the traditional need for IT administrators to manage compute resources.

- **Disaster recovery:**
  Data loss is a concern for every organisation. Storing data in the cloud guarantees that users can always access their data. With Cloud-based services, organisations can recover their data in the event of emergencies, such as natural disasters or power outages.

- **Pay as you go Pricing:**
  Instead of having to invest heavily in data centres and servers, you can pay only when you consume computing resources, and pay only for how much you consume.

  - **Massive economies of scale:**
    Many Cloud providers have existing infrastructure in place. You will never have the same purchasing power as an established Cloud provider. They have their own servers, networking gear, and their own storage array. They also have the capacity to build more when necessary. And they pass those cost savings on to you.

  - **Elasticity - Stop guessing about capacity:**
    Companies can freely scale up as computing needs increase, and scale down again as demands decrease. You no longer have to guess the capacity you need Cloud can scale with your business needs with no long term contracts.

- **Increase speed and agility:**
  Due to its server-less architecture, it is able to scale infinitely with demand. But essentially this means you've got no virtual machines or physical machines. So the great thing about Cloud computing is that you can increase your speed and agility in moving into the Cloud.

- **No costs in running and maintaining data centres:**
  You no longer need to focus on managing physical infrastructure. You have the luxury of letting the service provider manage these costs for you.

- **Go global within minutes:**
  You can easily deploy your application in multiple regions around the world. This enables you to provide lower latency and a better experience for your customers at minimal cost.

CLOUD COMPUTING TYPES

- **Infrastructure as a Service (IAAS)**
  Infrastructure as a service provider hosts servers, storage and other individualised resources over the internet. IaaS offers a variety of storage and memory options for any workload need.

  This is where you manage the server, which can be physical or virtual, as well as the operating system. Usually, the data centre provider will have no access to your server.

- **Platform as a Service (PAAS)**
  Platform as a service is a model in which a third-party provider hosts app development platforms and tools on its own infrastructure, available to customers over the internet. PaaS models are used for general software development

  The Cloud service provider manages the underlying hardware and operating systems. You just focus on your applications. You do not manage the security, patching, updates and maintenance.

- **Software as a service(SAAS)**
  Most popular at the consumer level is Software as a Service, which is software distribution from a third-party provider. This makes applications available over the internet like Microsoft Office 365 for productivity and email.

  All you worry about is the software itself and how you want to use it. The SaaS provider will take care of the data centres, servers, networks, storage, maintenance and patching.

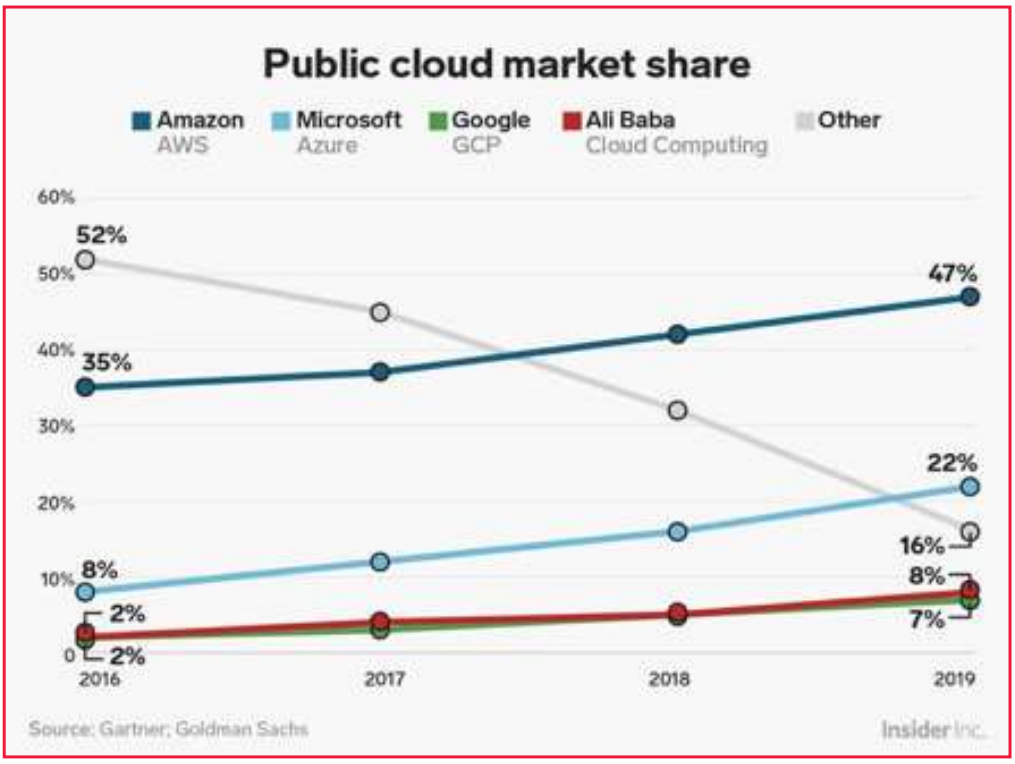
TYPES OF CLOUD COMPUTING DEPLOYMENTS

A Cloud can be private or public.

- Public Cloud – A public Cloud sells services to anyone on the internet like Amazon Website Services, Azure, Google Cloud Platform
- Hybrid – Mixture of public and private
- Private Cloud (or On Premise) – A private Cloud is a proprietary network or a data centre that supplies hosting services to a limited number of people, with certain access and permissions settings. You manage it, in your data centre. Eg. Openstack or vmware

Some service providers include Amazon Web Services, Microsoft Azure, IBM Cloud and Google Cloud Platform.

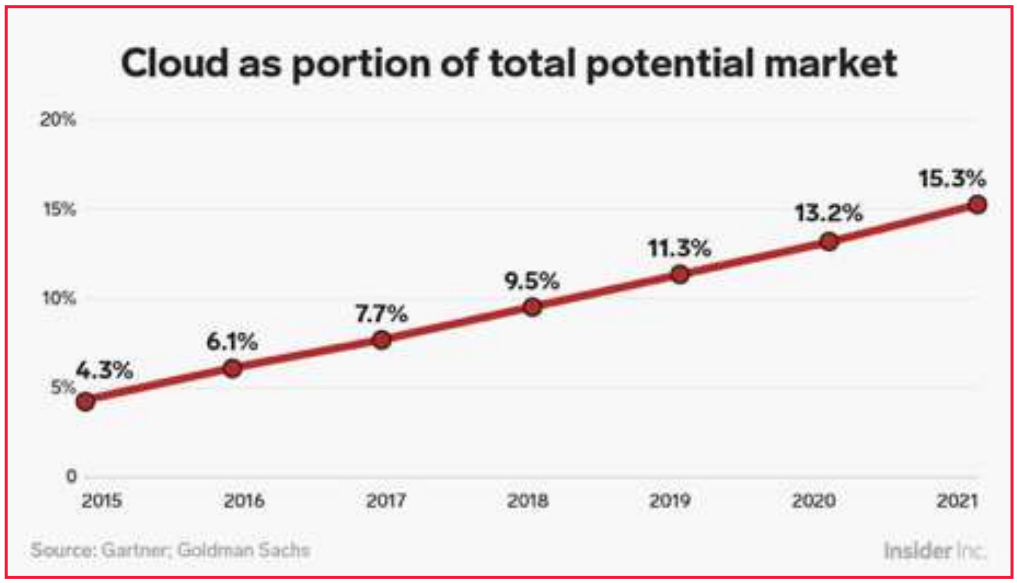
CLOUD SPEND AS PREDICTED BY GOLDMAN SACHS



Source: Business Insider

- Amazon are the clear market leaders in Cloud computing services. Companies are spending more and more on public Cloud and getting Cloud certified comes with great job security, as there are very few people who hold certifications specialising in Cloud computing.
- The Cloud-computing market should continue to grow at a rapid pace in the coming years, Goldman Sachs said in a report (2018).

  The market is dominated by four big firms: Amazon, Microsoft, Google, and Alibaba, so the opportunity for other players is rapidly closing, Goldman Sachs said.



- This graph essentially highlights, that in 2015, out of all the IT spend that organisations had, 4.3% was spent on Cloud computing. It is predicated to go all the way up to 15.3% in 2021.

REFERENCES

1. Tech Target, April 2020. Stephen J. Bigelow, Linda Rosencrance, "What is Cloud Computing, everything you need to know". https://searchcloudcomputing.techtarget.com/definition/cloud-computing
2. https://aws.amazon.com/what-is-cloud-computing/ Amazon Web Services, Inc. "What is Cloud Computing"
3. V. V. Arutyunov, Published: 26 October 2012. "Cloud computing: Its history of development, modern state, and future considerations"" https://link.springer.com/article/10.3103/S0147688212030082
4. Journal of computing and management studies ISSN 2516-2047. Issue 1. Volume 3. January 2019
5. T Aslam , "A review on Cloud Computing an Emerging Technology"
6. R P. Padhy, M. R. Patra, "Evolution of Cloud Computing and Enabling Technologies," International Journal of Cloud Computing and Services Science [IJ-CLOSER], October 2012
7. "Cloud Computing of E-commerce", Article in Modern Applied Science Vol. 13(1):27-35 · January 2019
8. Business Insider, Nov 2018, Samantha Lee "Goldman Sachs Cloud Computing Market Forecast" https://www.businessinsider.com/goldman-sachs-cloud-computing-market-forecast-aws-microsoft-azure-google-cloud-2018-11?IR=T

THE RISKS OF CLOUD COMPUTING

As per the work carried out by Dutta, Peng and Choudhary, there are four main categories and 12 sub-categories of the Cloud computing risk ontology (Dutta, Peng, & Choudhary, 2013). These four main risks are broken down into Organisational Risks, Operational Risks, Technical Risks and Legal Risks, which we consider the forefront considerations when understanding Cloud computing. All risks that impact considerations over a Cloud computing environment stem, or fit, into one of these categories. The first step in assessing this, is to evaluate whether a Cloud computing solution is being managed by the in-house staff or whether this will be managed by a third-party.

Organisational Risk

Organisations need to consider and take the proactive effort in ensuring that organisational risk is mitigated, ensuring current governance and compliance cover the Cloud environment. Organisational risk should be meticulously understood, over and above the IT implications. An adequate risk mitigation strategy needs to be developed and followed to protect the data and applications hosted in the Cloud environment (Dutta, Peng, & Choudhary, 2013). Policies and plans need to be implemented to manage the Cloud environment in order to meet the standards of industry governing bodies, local laws and regulations and audit standards. These would need to relate to the critical risk factors determined through risk assessments performed and ensure that these meet the audit standards required (Dutta, Peng, & Choudhary, 2013). This should not become an exercise of satisfying the IT audit controls, rather preventing loss of control and governance.

The most prevalent regulation within a South African setting would be the South African Protection of Personal Information Act (POPIA). This act aims to regulate the collection and processing of personal information collected by an organisation related to any information that identifies an individual (Mujinga, 2013). The main risk around the POPIA is the transferring of personal information to parties outside South Africa, where organisations may not necessarily receive guarantees that their Cloud Service Provider is compliant with these regulations (Mujinga, 2013). It is important for an organisation to have the correct controls or safeguards around their internal Cloud servers or their hosted data through a Cloud service provider in order to protect customer data collected as well as ensure this is kept in South Africa.

An organisation always needs to consider reputational risk, business resiliency and the IT specialists when selecting a Cloud service provider. These factors play a crucial role to the organisation to ensure that the Cloud service provider has the IT specialists to provide and maintain the service, the provider will not detriment the reputation of the organisation and the provider will be resilient in the long run as switching between providers can be a costly exercise. When using internal Cloud services, the organisation also needs to consider the in-house IT specialists and whether they will be able to develop, host and maintain a Cloud service relied on.

Operational Risk

The workings carried out by Carroll, van der Merwe and Kotzé noted that the second to most critical risk within a Cloud environment is third-party vendors (service providers) (Carroll, van der Merwe, & Kotzé, 2011). The biggest operational risk is service-level agreements (SLAs) over the Cloud environment and this ties in directly with the third-party risk as most organisations use outsourced Cloud servers to host their data. Considering this risk factor, organisations need to take pragmatic approach to be actively involved with the design and implementation of IT policies and Service Level Agreements (SLAs). As most organisations tend to outsource their Cloud solutions or data hosted within a Cloud environment, verifying the supplemented systems becomes difficult and thus assurance such as a SOC 1, 2 or 3 reports may be necessary (Mosher, 2011). This would provide assurances over the functionality and controls over the systems outsourced, where further monitoring should be performed over the SLAs in place with the vendors to ensure stringent controls are in place over the activities performed by them (Mosher, 2011).

Often, organisations underestimate the costs of implementing a Cloud solution whether it be in-house, or vendor managed. Additional costs from an in-house developed Cloud solution could come down to the lack of planning or risk assessments performed over the environment. This could stem to regulatory breaches which would lead to fines and lawsuits, furthermore inappropriate planning could lead to mismanagement of maintenance over the Cloud environment. When referring to an environment managed by a Cloud service provider, hidden costs are often incurred by the organisation (Dutta, Peng, & Choudhary, 2013). These are usually in the form of disaster recovery costs, application configuration fees and data loss insurance. This is where the importance of managing the risk associated to the SLA become important. Service fees charged by the Cloud service provider may gradually increase over time and leaves the organisation in a difficult situation as the risks and costs of switching providers may outweigh the fees being charged.

Usability of the Cloud computing service becomes the final operational risk, which encompasses both the users on the Cloud platform and the service reliability. Like any new system being introduced into an IT environment, one will always face user resistance to adopt the system, and the mandatory process of upskilling staff to be able to use the system. Managing user resistance against a Cloud computing system, like all systems, comes down to the application of different management styles being applied across an organisation (Shang & Su, 2004). Overcoming the resistance against the change of implementing a Cloud solution is the first step, this then needs to be followed by training and upskilling of users as to the Cloud solution implemented, without this would lead to further resistance or failure of the Cloud solution implemented. It is therefore as important to manage the personnel and users that will be using the Cloud solution. The second component comes down to the Cloud solution reliability which talks to both the down-time of the solution as well as the resources allocated to the solution and its maintenance (Dutta, Peng, & Choudhary, 2013). Although a Cloud solution may be implemented successfully, maintenance needs to be managed with regulated plans and policies for when the system is experiencing down-time, problems or incidents and the resolutions thereof. Resources need to be carefully planned in order to avoid under- or over-staffing of the Cloud solution.

Technical Risks:

System performance and integration are integral in the planning, implementation and maintenance over a Cloud solution in one's IT environment. System performance refers directly to the factors affecting the performance of the Cloud solution and includes network speeds, the database size and the hardware capacity required (Dutta, Peng, & Choudhary, 2013). These play a critical role in determining the viability of implementing a Cloud-based solution and the infrastructure required. The second component of system performance would be the number of users that would be using the system, both from the off-set and users that would be migrated to the solution in future iterations. This would directly impact both the IT access management controls currently in place and needed, and the traffic experienced on the system. This extra traffic may require adjustments to the infrastructure supporting the Cloud-based solution. System performance ties into both budgets for the implementation of a Cloud solution (whether it be an in-house or vendor-based solution) and the infrastructure to support this solution. System integration refers to the integration of the new Cloud-based solution with the current legacy applications, current Cloud-based solutions, and third-party systems. One needs to carefully consider the risks associated to the detailed specifications of implementing a new system within the IT environment considering current systems, operating systems and databases. Interfaces, data flows and process understandings need to be carefully considered to map out the in-depth integration of a new Cloud-based solution amongst already existing systems. If the Cloud-based solution acts as a replacement for an already existing system, then data migrations need to be considered.

Data quality, integrity and security are at the forefront of technical risks that need to be considered when dealing with critical data in a Cloud-based solution. One needs to consider that when using a Cloud service provider, it may be more difficult to manage the protection over the data as the organisation does not have direct control over data being hosted elsewhere (Carroll, van der Merwe, & Kotzé, 2011). This is again down to the management of the third-party vendor, the service-level agreement in place and assurance testing performed by the organisation of the third-party data protection controls. Data fragmentation or loss can be caused by the multiple Cloud applications within ones IT environment (Dutta, Peng, & Choudhary, 2013), whereby regular back-up processes need to be performed within an organisation. These back-ups, alongside the regular recovery tests performed, ensures that the data backed-up can be restored appropriately: it would overlay protection against data loss, unwanted data overwrite, or destruction of data (Carroll, van der Merwe, & Kotzé, 2011). The risk of data being unavailable due to reliance placed on internet connections between data transfers and data processing is a prominent problem which should be addressed through the system performance assessments.

Data integrity is affected by the patch management policies, procedures and practices. Without these the networks, applications and databases, an environment become vulnerable (Carroll, van der Merwe, & Kotzé, 2011). Access management, privileged user access rights and change management over any database becomes critically important to assess when regarding the integrity of data. One needs to carefully manage who has access to make changes directly to any dataset and any controls or assurances one can obtain to ensure that no one can make unauthorised changes to data. If the Cloud solution is an in-house solution, stringent controls need to be in place to ensure that no one can or has made unauthorised changes to a dataset or the database. Likewise, with a third-party based Cloud solution, it is not enough to purely rely on a service-level agreement. Assurance testing will need to be performed to ensure that this data is being protected against unauthorised changes. Data security refers to the current encryption techniques against cyber threats, which has been comprehensively covered in the proceeding sections.

Legal Risks:

Like all IT systems and environments, legal regulations and formalities need to be considered with regards to a Cloud-based solution. As discussed in previous sections, POPIA is at the forefront for legal risks associated to the privacy of user's data. Matters such as the information allowed in the Cloud should be identified and managed appropriately (Carroll, van der Merwe, & Kotzé, 2011). One cannot simply rely on SLAs or the fact that the Cloud solution and data associated with this solution are managed by a third-party. In-depth audits need to be performed over the third-parties environments in order to obtain assurance that there are no legal breaches regarding data privacy regulations. Regular reviews over current governance plans and policies should be performed to ensure that these are abiding to laws and regulations. If the Cloud solution and data is being managed by a third-party it is critical that one has critically assessed the intellectual property regulations for the organisations data. This would avoid sharing protected client data, business data, business processes and IT infrastructure of the organisation. The last consideration with regards to legal risks is contracts. It is important to always consider the binding contract between an organisation, its employees and a third-party vendor (where a Cloud-based solution is outsourced).

REFERENCES

Carroll, M., van der Merwe, A., & Kotzé, P. (2011). *Secure Cloud Computing- Benefits, Risks and Controls.*
Dutta, A., Peng, G. A., & Choudhary, A. (2013). Risks in Enterprise Cloud Computing: the Perspective of IT Experts. *Journal of Computer Information Systems, 39-48.*
Mosher, R. (2011). Cloud Computing Risks. *ISSA Journal, 36-37.*
Mujinga, M. (2013). Privacy and Legal Issues in Cloud Computing - The SMME Position in South Africa. *Australian Information Security Management Conference, 49-59.*
Shang, S., & Su, T. (2004). Managing User Resistance in Enterprise Systems Implementation. *Americas Conference on Information Systems* (pp. 149-153). New York: Association of Information Systems.

CYBER RISKS:

The adoption to Cloud Technology encompasses numerous risks. In order to be secure and ensure service continuity, fault tolerance should be in place. Companies such as Amazon Web Services provide fault tolerance methods such as redundancy by implementing load balancing. Byzantine Fault tolerance, one of the most popular methods of fault tolerance, is also advised.

"Redundancy, as a solution to achieving fault tolerance, was introduced by John von Neumann in the 1950's and has proven to be successful (Han et al., 2005). However, the development of Cloud Technologies and advancements in hardware and software components, have allowed for new and improved methods of implementing redundancy with a multitude of faults (Cheraghlou, Khadem-Zadeh and Haghparast, 2015). Advancements in consensus-based technologies also indicate possibilities of implementing revised Byzantine Models (Block Chain will assist in this)" (Christopher O'Flaherty et al). However, fault tolerance is not the only remedy to cyber threats in Cloud computing.

Before determining the remedies to the numerous cyber threats, it is important to be aware of all possible cyber risks and threats.

Further cyber threats/risks include[1]:

- Malware infections: owing to the fact that the Cloud is constantly connected to the internet, several threats exist.
- Distributed Denial of Service (DDOS) and Denial of Service (DOS) attacks are popular attacks against Cloud services and disrupt service continuity.
- Crypto jacking: owing to the growth of cryptocurrency, hackers use your computer resources to process cryptocurrency transactions by installing a crypto mining script on your servers without consent. This significantly slows down systems and servers.
- Data breaches occur when unauthorised users gain access and can view and transmit data.
- Data losses: Similar to data breaches however these often occur due to natural, or maliciously induced, disasters. Large pools of data can be lost.
- Insider threats: Employees may cause privacy violations or fall target to social engineering. Employees may also introduce malware through bringing their own devices.
- Hijacking accounts: through dumpster diving or shoulder surfing, or simple passwords, account hijacking occurs through a hacker gaining a users' log in credentials.
- Insecure applications.
- Inadequate training of staff – whether it be on how to accurately use a tool, or awareness of cyber risks.
- Third party services may have their own vulnerabilities. For example, IoT devices have numerous weaknesses and may lead to intrusion and attack. Insecure API's my also aid data breaches.

To mitigate these risks, it is recommended to follow cybersecurity Cloud best practices which include[2]:

- User Access Control.
- SSH Keys to ensure secure connection – key management policies should thus be communicated and emplaced.
- Multi-factor Authentication.
- Monitoring of logs and configurations.
- Patch Management.
- Vulnerability assessments.
- Employee awareness.
- Edge computing for IoT devices.
- Disaster management plans.
- In networking architectures, fundamental security protocols are necessary including IDPS's (Intrusion detection and prevention systems) and firewalls.

Threat detectors are necessary as well as anti-virus software and shields to protect from threats such as DOS and DDOS attacks.

The implementation of the following policies have thus gained popularity:

A BYOC (Bring your own Cloud) policy: This would state the requirements should an employee want to use a Cloud service.

A BYOD (bring your own device) policy: This would state the requirements should an employee wish to use their own device.

[1]https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/
[2]https://wire19.com/10-biggest-threats-to-cloud-computing-2019-report/

CONCLUSION:

It is evident that the Cloud is a game changing technology revolutionising how business is conducted. The Cloud is utilised with various other emerging technologies including IoT, Big data, and numerous others. However, with innovation, comes a multitude of risks. To not account for these risks can lead to detrimental consequences and thus having a third party institution aid in this process may guarantee the success of Cloud adoption.

WE TAKE IT PERSONALLY.
FOR FURTHER INFORMATION, CONTACT:

SCOTT HEWITT
BDO Financial Services Technology Senior Analyst
shewitt@bdo.co.za

RESHELLE NAIDOO
BDO Financial Services Technology Junior Analyst
resnaidoo@bdo.co.za

CHRISTOPHER O'FLAHERTY
BDO Financial Services Technology Junior Analyst
coflaherty@bdo.co.za

NEVELLAN MOODLEY
Head of BDO Financial Services Technology
nmoodley@bdo.co.za

/BDOSouthAfrica


/bdoafrica


/bdo_sa


/company/bdo-south-africa

www.bdo.co.za