



Cloud outsource directive and guidance note issued by the South African Reserve Bank

 by **Isaivan Naidoo**

 ▲
[click to print this article](#)

Cloud computing and offshoring of data is no longer a taboo among banks. It is becoming a necessity and is the current definitive trend. However, the South African Reserve Bank (“**SARB**”) has issued a directive and guidance note detailing items banks must consider when electing to adopt cloud computing as a service or any offshoring of data.

At the outset, the SARB requires that banks elect a risk based and mitigation approach, having consideration to the bank’s risk profile, size of the bank and its operations. For the purposes of this article, we will only highlight some of the critical provisions to consider, namely banks are directed to:

1. ensure that they have in place a formal board-approved data strategy and governance framework;
2. ensure that the offshoring of data and use of cloud computing in no way inhibits any regulators’ ability to fulfil their duties; and
3. ensure that any cloud computing arrangement does not prevent the bank’s ability to conduct forensic audits or investigations.

Banks must also consider the classification of data, materiality of the activity outsourced, level of risk, mode and form of cloud computing and offshoring of data. A banks data strategy should include at the very least:

1. the manner in which the bank classifies its data;
2. in which jurisdictions may the data be stored;
3. which service and deployment models are applicable to the classifications of data;
4. which security requirements will apply to the different data classifications; and
5. the process in respect of the bank’s data loss and breach requirements.

Put simply, the bank must put in place a strategy as well as formal policies and robust contracts to ensure that the service provider rendering the cloud services or offshoring of data takes steps to assist the bank in its compliance efforts. Some of the suggested proactive steps that banks should adopt are set out below:

1. first, conduct a due diligence of the supplier, know your supplier, cut through the sales talk and glossy marketing material;
2. review the contract terms and ensure that such terms address, *inter alia*, data security, data sovereignty, security standards, data backups, audit rights and data recovery in addition to other negotiated terms that are best practice for cloud transactions;
3. scrutinise the vendor’s standard terms; do not just accept what is presented without checking how the vendor will assist with ensuring that the bank remains compliant. This is also in keeping with sound IT corporate governance;
4. ensure acute awareness of what data is being processed or offshored. This can only be accomplished by implementing an enterprise wide sound data strategy; and
5. ensure, as a bank, that sound policies and procedures exist in order to benchmark any vendor cloud offering against not only the aforementioned directives, but also against the bank’s own risk appetite.

ENSafrica’s specialist TMT team can assist in your bank’s compliance initiatives, drafting of standard policies and procedures as well as ensuring that sound contracts are put in place with cloud service providers.

For more information, please contact:



Isaivan Naidoo

technology, media and telecommunications | director

cell: +27 82 310 5172

No information provided herein may in any way be construed as legal advice from ENSafrica and/or any of its personnel. Professional advice must be sought from ENSafrica before any action is taken based on the information provided herein, and consent must be obtained from ENSafrica before the information provided herein is reproduced in any way. ENSafrica disclaims any responsibility for positions taken without due consultation and/or information reproduced without due consent, and no person shall have any claim of any nature whatsoever arising out of, or in connection with, the information provided herein against ENSafrica and/or any of its personnel. Any values, such as currency (and their indicators), and/or dates provided herein are indicative and for information purposes only, and ENSafrica does not warrant the correctness, completeness or accuracy of the information provided herein in any way.

info@ENSafrica.com
level 2 BBBEE rating (South Africa)

