South African Reserve Bank

Prudential Authority

Ref.: 15/8/2

D3/2018

To: All banks, controlling companies, branches of foreign institutions and auditors of banks or controlling companies

Directive issued in terms of section 6(6) of the Banks Act 94 of 1990

Cloud computing and the offshoring of data

Executive summary

Regulation 39 of the Regulations relating to Banks (Regulations) requires banks, controlling companies and branches of foreign institutions (hereinafter collectively referred to as 'banks') to establish and maintain an appropriate process of corporate governance. This process includes the maintenance of effective risk management processes by banks and the continuous management of risk arising from the use of cloud computing and/or the offshoring of data.

This directive sets the Prudential Authority's requirements and related considerations for cloud computing and/or the offshoring of data and should be read with Guidance Note 5/2018.

1. Introduction

1.1 The Prudential Authority (PA) is aware that there are banks which may already offshore their data, for instance, through an insourcing relationship with a parent organisation. In addition, banks are increasingly considering extending their use of cloud computing to more significant activities.

1.2 In this regard, the PA would like to clarify its policy and regulatory stance with regard to cloud computing and/or the offshoring of data.

1.3 For the purpose of this directive:

1.3.1 Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage facilities, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

1.3.2 Offshoring of data refers to the storage and/or processing of data outside the borders of South Africa.

1.4 The purpose of this directive is to set out the PA's requirements under which banks may use cloud computing and/or offshore their data.

1.5 The supplementary information contained in Guidance Note 5/2018 is provided to assist banks to comply with and better understand the PA's requirements with regard to cloud computing and/or the offshoring of data. As such, this directive should be read in conjunction with the aforesaid Guidance Note 5/2018.

1.6 Banks should consider the contents of this directive and the associated Guidance Note 5/2018 in the context of their overall legislative obligations, including obligations to the Financial Intelligence Centre (FIC) and the South African Reserve Bank's Financial Surveillance Department, which may have different statutory objectives and requirements.

1.7 The PA expects banks to follow a risk-based approach that is aligned with the bank's risk appetite, based on the nature and size of its operations, when implementing cloud computing and/or the offshoring data.

1.8 Different cloud models implemented by banks should be assessed based on the level of risk and/or whether mitigation controls, or part thereof, are managed either internally, externally and/or through a combination of both.

2. Directive

2.1 Based on the aforesaid, and in accordance with the provisions of section 6(6) of the Banks Act 94 of 1990, banks are hereby directed to:

2.1.1 comply with the requirements as set out in this directive in which banks may make use of cloud computing and/or the offshoring of data, read in conjunction with the related Guidance Note 5/2018, from 1 October 2018 onwards;

2.1.2 provide the PA with the information related to their material cloud computing and/or offshoring of data arrangements, in accordance with Guidance Note 5/2014; and

2.1.3 refer any uncertainty in respect of any matter referred to in this directive to the PA for further clarification, as deemed necessary.

2.2 The directive under which banks may use cloud computing and/or the offshoring of data are set out below:

2.2.1 Banks must have in place a formally defined and board approved data strategy and data governance framework.

2.2.2 Banks that use cloud computing and/or offshore their data must have a clearly defined policy for such activities, which is aligned with its business strategy and linked to its risk appetite.

2.2.3 Oversight of cloud computing and/or the offshoring of data must be incorporated into the governance structures, processes and procedures within the bank.

2.2.4 Banks must ensure that their risk and control frameworks, including the application thereof, are designed and operating effectively in order to manage the risks associated with the use of cloud computing and/or the offshoring of data.

2.2.5 Prior to undertaking a particular cloud computing and/or data offshoring initiative, the bank must assess whether the risk involved is within its risk appetite.

2.2.6 All strategic investments by the bank, including the use of cloud computing and/or the offshoring of data, must be subjected to appropriate due diligence.

2.2.7 Banks must take all reasonable measures to ensure the confidentiality, integrity and availability of its data, information technology (IT) applications or systems.

2.2.8 Banks that use cloud computing and/or offshore their data must ensure that they remain compliant with applicable legislation and regulations, both locally as well as in any country where the cloud services and/or data are hosted.

2.2.9 The use of cloud computing and/or the offshoring of data must not in any way infringe on the bank's supervisors or prevent any regulatory mandated access to information, nor must it impact on its regulators' ability to fulfil their duties.

2.2.10 Banks must have contingency plans to continue with operations and meet their core obligations, such as regulatory, statutory or otherwise, despite any cloud computing and/or offshoring of data arrangements which may be in place.

2.2.11 Banks must ensure that their intellectual property rights and contractual rights to data are not compromised, despite any cloud computing and/or offshoring of data arrangements which may be in place. Data must always be in a usable, readable and portable state, even when the contract is terminated.

2.2.12 Any cloud computing and/or offshoring of data arrangements must not impact on banks' ability to conduct forensic audits or investigations.

2.2.13 All cloud computing and/or offshoring of data arrangements must be contained in a documented, legally binding agreement.

3. Acknowledgement of receipt

3.1 Kindly ensure that a copy of this directive is made available to your institution's independent auditors. The attached acknowledgement of receipt duly completed and signed by both the chief executive officer of the institution and the said auditors should be returned to the PA at the earliest convenience of the aforementioned signatories.

Kuben Naidoo
Deputy Governor and CEO: Prudential Authority

Date: 5 SEPTEMBER 2018

The previous directive issued was Directive 2/2018 dated 13 August 2018.