South African Reserve Bank
Prudential Authority

Ref.: 15/8/2

G5/2018

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

Guidance Note issued in terms of section 6(5) 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 as well as the continuous management of risk arising from the use of cloud computing and the offshoring of data.

Banks are allowed to make use of cloud computing and to offshore data as long as they remain in compliance with the relevant requirements specified by the Prudential Authority and other regulatory and supervisory authorities as set out in applicable laws. The ultimate responsibility for ensuring that the risk surrounding cloud computing and the offshoring of data are managed vests with the relevant bank's board of directors.

This guidance note is issued to assist banks to meet the Prudential Authority's requirements with regard to cloud computing and/or the offshoring of data as set out in Directive 3/2018. As such, this guidance note should be read in conjunction with Directive 3/2018.

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 guidance note:

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 This guidance note contains supplementary information that will assist banks to meet the PA's requirements with regard to cloud computing and/or data offshoring. It should therefore be read in conjunction with the aforementioned directive.

1.5 This guidance note and the accompanying Directive 3/2018 should not be seen as exhaustive and should therefore not be read in isolation. Banks should consider the requirements set out in Directive 3/2018 as well as the guidance set out in the guidance note in the context of their overall legislative obligations, including obligations to the Financial Intelligence Centre (FIC) and the South African Reserve Bank's (SARB) Financial Surveillance Department, which may have different statutory objectives and requirements.

2. Applicability of this guidance note

2.1 This guidance note addresses both the use of cloud computing and/or the offshoring of data. These activities may be related but may also be independent of each other. It is therefore possible for a bank to make use of a cloud service provider (CSP) where its data is hosted in South Africa, while it is also possible for a bank to have its data centres outside of the borders of South Africa without making use of cloud computing.

2.2 The requirements as set out in Directive 3/2018 are principle-based; therefore, this guidance note is intended to assist banks in evaluating key considerations to give effect to the requirements as set out in the aforesaid directive. How the respective requirements are addressed will include, but not be limited to, the classification of data, materiality of the outsourced activity or process, level of risk involved, model of cloud computing and/or the offshoring of data used. For instance, an on-premise private cloud hosted by a bank containing public data has inherently less risk than personal data or core banking services hosted in a public cloud run by a CSP in a foreign jurisdiction.

2.3 The PA expects banks to follow a risk-based and a principle-based approach, aligned with their overall business strategy, in implementing measures to address their requirements to engage in cloud computing and/or the offshoring of data.

3. Existing guidance and requirements

3.1 The considerations set out in this guidance note do not supersede any previously issued or specified guidance or requirements, such as Guidance Note 5 of 2014 (G5/2014). This guidance note is meant to complement existing guidance and regulatory requirements. As set out in paragraph 4.5 of G5/2014, the PA would like to emphasise that banks should appreciate the significance of cloud computing initiatives and the offshoring of material information technology (IT) business activities and functions.

4. Considerations

4.1 Guidelines for compliance with paragraph 2.2.1 of Directive 3/2018 requiring that 'banks must have in place a formally defined and board approved data strategy and/or data governance framework'.

4.1.1 The data strategy/framework should include:

a. how a bank classifies its data;
b. where (in which jurisdictions) data may be stored (data residency);
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; and
e. the process in relation to bank's data loss and breach requirements.

4.1.2 Banks should maintain a register of all their information assets, including data, IT applications, systems and processes. All such assets should be classified according to the bank's data classification policy. The location of the data should also be noted and should be in line with data residency requirements as well as information security requirements.

4.1.3 The data strategy should be reviewed periodically in line with the bank's policy requirements, taking all relevant legislative and regulatory requirements of other relevant authorities in South Africa, such as the Information Regulator of South Africa and the FIC, into consideration.

4.1.4 Banks should have clearly defined data loss and breach processes, including notification and escalation to relevant stakeholders.

4.2 Guidelines for compliance with paragraph 2.2.2 of Directive 3/2018 requiring that 'banks that use cloud computing and/or offshore their data must have a clearly defined policy for such activities, which is aligned to its business strategy and linked to its risk appetite'.

4.2.1 Cloud computing and/or offshoring of data policy considerations

a. Refer to paragraph 6.2 of G5/2014 for additional guidance with regard to outsourcing policies.
b. The policy should be aligned with the bank's risk appetite for such activities, including due consideration of the bank's data policy.

c. A cloud computing and/or offshoring of data policy should take into consideration, among other things, change management and the desired architecture and operating model.
d. The use of cloud computing and/or the offshoring of data should not only be driven by cost factors in isolation but should also consider wider disciplines in the bank, including enterprise architecture and information security.
e. A cloud computing and/or offshoring of data strategy should, among other things, define the benefits and the risks involved in such activities.
f. The bank's decision-making structures and governance processes should be supported by the cloud computing and/or offshoring of data strategy.
g. Where cloud computing and/or the offshoring of data occurs through an outsourcing arrangement, the cloud/data offshoring strategy should be aligned with the bank's outsourcing policy.

4.2.2 The bank should have a clear understanding of the benefits and risks involved in cloud computing and/or the offshoring of data. The policies should specify the management of the risks in order to maximise the benefits through effective end-to-end governance practices.

4.3 The guidelines for compliance with paragraph 2.2.3 of Directive 3/2018 require that 'oversight for cloud computing and/or offshoring of data must be incorporated into the governance structures, processes and procedures within the bank'.

4.3.1 Accountability

a. As specified in regulation 39(1) of the Regulations the board of directors (board) of a bank is ultimately responsible for establishing corporate governance within the bank and it may appoint supporting committees to assist it with its responsibilities. In line with regulation 39(3) of the Regulations, these responsibilities include the continuing management of, among other things, the following risks: counterparty risk; country risk and transfer risk; operational risk; risk arising from the outsourcing of material business activities and functions; and technology risk. In accordance with regulation 39(4) of the Regulations, the bank should have comprehensive risk management processes, practices and procedures as well as board-approved policies in place.
b. The board retains ultimate responsibility for the use of cloud computing and/or the offshoring of data. The use of service providers does not relieve the board and senior management of their responsibility to ensure that cloud computing and offshoring activities are conducted in a safe and sound manner and in compliance with all relevant legislation.
c. Banks' senior management is responsible for ensuring that the cloud computing and/or offshoring of data activities are appropriately executed, including overseeing the development and implementation of risk management and reporting programmes. The senior management of the bank should ensure ongoing monitoring of services and service providers, respond to issues when identified, and escalate significant issues to the board.

d. The senior management of the bank retains ultimate responsibility for ensuring that the PA and other stakeholders, such as the banks' external auditors, have access to required information to enable them to exercise their respective duties under the Financial Sector Regulation Act 9 of 2017, the Banks Act 94 of 1990 and other relevant legislation.
e. Also refer to paragraph 6.1 of G5/2014 for additional guidance on board and senior management oversight as well as other related responsibilities for outsourcing.
f. Decision-making and oversight responsibilities with respect to cloud computing and/or the offshoring of data should be duly documented and approved according to bank procedures.
g. The senior management of the bank should ensure that it is clear about what service is being provided and that responsibility and accountability between the bank and its service providers is clearly delineated.

4.3.2 Managing and monitoring the relationship

a. Refer to paragraph 6.6 of G5/2014 for additional guidance regarding the management and monitoring of outsourcing relationships.
b. The bank should have adequate procedures and systems in place that enable it to measure and track the risk versus benefit of any cloud computing or offshoring initiative.
c. The bank should develop and maintain operational and strategic oversight mechanisms which enable the ongoing assessment of performance against agreed service levels, the viability of the service and/or service provider, identification of a change in the relationship, and a timely response to arising issues and emerging risks.
d. Banks should manage services and service providers proactively by regularly receiving timely and sufficient information to enable effective oversight.
e. Oversight should include monitoring the alignment of the cloud computing and/or data offshoring service provider's environmental requirements compared to those required by the bank. This should include performance, capacity, security, resilience and recoverability requirements.
f. Responsibility for the day-to-day operations and strategic management of the services should be clearly allocated.
g. The senior management of a bank should ensure that the bank has processes and procedures in place to identify and deal with any weakness in a service provider's performance that may have an adverse impact on the service provided to the bank.
h. Cloud computing or offshoring arrangements which are no longer in line with expectations or the bank's strategic goals, objectives or risk appetite should be terminated.

4.4 Guidelines for compliance with paragraph 2.2.4 of Directive 3/2018 requiring that '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 data offshoring'.

4.4.1 Assurance

a. Banks should ensure that, where cloud computing and/or offshoring of data services are provided by third parties, the bank's assurance model provides assurance over all material activities at an appropriate level. The planning of assurance work should be risk-based, taking into account the materiality of services, risk appetite, level of risks involved and the classification of data, while addressing the bank's audit and assurance policies.
b. Additional assurance work may be triggered by material changes to cloud computing services, data being offshored or compliance requirements, including changes to associated threats and vulnerabilities.
c. Services provided by third parties outside of the control of the bank should also be covered in the assessment of the bank's audit universe and related assurance testing scheduled in order to asses all material aspects of the IT security control environment, both at the bank and at third parties, over time.
d. Refer to paragraph 6.10 of G5/2014 for additional guidance on the assessments of outsourcing.

4.5 Guidelines for compliance with paragraph 2.2.5 of Directive 3/2018 requiring that 'prior to undertaking a particular cloud computing or data offshoring initiative, the bank must assess whether the risk involved is within its risk appetite'.

4.5.1 Risk assessment

a. The risk assessment should identify all risks involved and determine whether adequate controls are in place, or can be implemented, in order for the initiative to be in line with the bank's risk appetite.
b. Risk assessments are required for all material outsourcing arrangements, according to G5/2014 (see paragraph 5.1 for key outsourcing requirements).
c. Refer to paragraph 6.3 of G5/2014 for additional guidance regarding planning and risk assessments related to outsourcing.
d. Banks should identify, assess, manage, mitigate and report on risks associated with cloud computing and/or the offshoring of data to ensure that they are able to continue to meet their operational and financial obligations to all stakeholders, including customers and regulators.
e. Risks should be adequately understood and managed prior to entering into a cloud computing or data offshoring arrangement. Factors that should be addressed include continuity, data protection, and prudential and regulatory compliance, and not infringe on the ability of supervisors to execute their prudential duties.
f. The risk assessment should be documented and provide management with sufficient information to be useful for decision making.
g. Responsibility should be assigned for managing the risks identified in the cloud computing and/or the offshoring of data initiative.

h. The risk assessment should be updated as part of monitoring and managing the outsourcing relationship. The bank should update its risk mitigation plans, where appropriate, based on the results of the risk assessment.

i. Part of the risk assessment should entail considering the sustainability of making use of cloud computing and/or the offshoring of data as well as implications for reverting to prior arrangements.

4.5.2 The bank should consider where, how and by whom the services are provided. The use of subcontracting and different jurisdictions should not impact on the bank fulfilling its duties to all its stakeholders, including data residence requirements.

4.5.3 The impact of using different jurisdictions should be considered in the light of the bank's data strategy as well as the potential impact on the role of the supervisor and its access to data.

4.6 Guidelines for compliance with paragraph 2.2.6 of Directive 3/2018 requiring that 'all strategic investments by the bank, including the use of cloud computing and/or offshoring of data, must be subjected to appropriate due diligence'.

4.6.1 Due diligence and selection

a. Banks should consider the applicability of G5/2014 on the outsourcing of material activities of banks.

b. Refer to paragraph 6.4 of G5/2014 which sets out additional guidance for due diligence and selection surrounding outsourcing to service providers.

c. The senior management of a bank should ensure that the particular service provider is committed to providing, and is able to provide, the required service at agreed levels for the duration of the arrangement.

d. The strength of the service provider's governance, risk and compliance environment should also be assessed before entering into a contract. With the use of cloud computing and/or data offshoring, security controls surrounding the management of data is of critical importance.

e. The depth of due diligence undertaken should be commensurate with the criticality and/or sensitivity of the data and activities/functions involved as well as the level of trust placed on the service provider. Factors to consider regarding the depth and formality of the due diligence performed include the risks involved, scope, complexity, materiality of the business activity or function, and the reputation and industry standing of the service provider.

f. All investments should adhere to the appropriate governance processes to ensure the strategic fit and business readiness.

g. Where a bank makes use of a third-party service provider to provide cloud computing services and/or to offshore data, the bank should have developed a list of reputable service providers which are to be analysed as part of a due diligence process prior to making the final selection. This should also support the planning of the business continuity processes since the bank should be able to identify whether there are any viable alternatives to the preferred service provider.

4.6.2 Business case

a. Banks should have a valid and documented business case for each instance of moving IT services to the cloud computing and/or for the offshoring of data. The business case should clearly identify the link between cloud computing and/or data offshoring and the manner in which it supports the business strategy of the bank.
b. The business case should clearly define the expected benefits and how these are to be measured.
c. The business case should contain a cost versus benefit analysis.
d. The business case should indicate how the bank's data strategy is addressed, for instance, in terms of the classification of data as well as data residence.

4.6.3 Stakeholders

a. Input should be obtained from all relevant stakeholders to ensure strategic alignment within the bank, for instance, with the IT department, including enterprise architecture and information security, and the risk department, including IT risk.
b. The bank should identify all relevant stakeholders who may, further to the above examples, include compliance, finance, internal audit and legal, and who should provide input into or have sight of the business case.
c. Banks should, as part of considering cloud computing and/or offshoring initiatives, obtain an understanding of the interdependencies in its enterprise and application architecture.
d. Banks should involve information security and security architecture subject matter experts in the design of cloud-based and offshoring solutions.
e. Banks should consider the impact of cloud computing and/or data offshoring on its configuration management as well as its IT provisioning processes.

4.6.4 Prior to engaging in a cloud computing initiative or offshoring of data, the bank should assess its readiness. The assessment should entail a full understanding of the data, services and processes affected, and assess whether the existing impacted business operations are capable and ready for the change. The assessment should identify any gaps and integration requirements which are to form part of the implementation of the cloud computing services and/or the offshoring of data.

4.7 Guidelines for compliance with paragraph 2.2.7 of Directive 3/2018 requiring that 'banks must take all reasonable measures to ensure the confidentiality, integrity and availability of its data, IT applications or systems'.

4.7.1 Part of the risk assessment of a cloud computing and/or offshoring of data engagement should include an information security risk assessment in order to determine the necessary security controls to be implemented in line with the bank's risk appetite, irrespective of where the services are provided. Security assessments should be updated periodically, such as after a material change, and be in line with the bank's policy requirements.

4.7.2 Banks should comply with all relevant information security standards and legislative requirements of South Africa. One such example is the requirement surrounding the transfer of personal information outside of the Republic of South Africa as set out in Chapter 9 of the Protection of Personal Information Act 4 of 2013 (POPI Act). Specific reference is made to the requirements surrounding an adequate level of protection having to be provided by a third party, which are substantially similar to the requirements of the POPI Act itself.

4.7.3 Information security assessment

a. Factors to be considered in assessing the adequacy of information security controls include:
   i. the materiality of the IT systems;
   ii. nature of the process or activities involved;
   iii. the classification of data;
   iv. third parties involved;
   v. the location of the data; and
   vi. the cloud deployment model.

b. Risks should be clearly described and at a level of granularity which allows for a meaningful understanding of the actual risk and identification of specific mitigating controls (including any required remediation actions).

c. The use of scenario analysis to contemplate plausible security events (including a loss of availability) may be useful in aiding the understanding of the risks involved with the arrangement.

d. The strength of the control environment should be appropriate for the risks involved in the arrangement. An understanding of the nature and strength of controls required may be strengthened through initial and periodic assessments (such as after a material change) of the design and operating effectiveness of implemented controls.

4.7.4 Information security considerations

a. Banks should obtain assurance from third parties involved and contractually agree that third parties will adhere to the information security requirements defined by the bank. The information security requirements should, for instance, deal with patch management, authentication, authorisation and administration.

b. Banks should agree data loss and breach processes with any third party involved, and ensure they are aligned with the bank's risk appetite and legal as well as regulatory obligations.

c. Contractual agreements should clearly define accountability and penalties in cases where controls are breached, including who would be responsible for losses resulting from a data breach.

4.7.5 Assurance and testing

a. The contractual agreement with any third party involved should specify how the bank will verify adherence to the agreed information security requirements. This may include, but not be limited to, third-party assurance audits as well as any other security testing requirements such as vulnerability scanning and penetration testing.

b. Banks should obtain a copy of the information security policy of any third parties involved in order to determine whether it contains adequate provisions for security standards and controls which would be in line with the bank's service level agreement (SLA) with the third party.

4.7.6 Security standards

a. Banks should be aware of the information/security technology governance and control frameworks or standards that any third party involved in cloud computing and/or the offshoring of data adheres to. It should further be aware of whether the third party is certified or audited in terms of any of these, and should obtain assurance through obtaining copies of audit/assurance reports on adherence.

b. Although standards are still maturing and best practices are not yet fully established, banks should consider leading standards and control frameworks provided by reputable institutions such as National Institute of Standards and Technology (NIST), the Canadian Standards Association (CSA) and the Information Systems Audit and Control Association (ISACA).

c. Agreed security requirements should include physical security standards at the third party's data centres which should not be less stringent than the physical security measures that would have been in place had the data been hosted at the bank's own data centres.

4.7.7 Access rights

a. Access rights to information assets in the cloud or offshored data should be restricted in line with the bank's user access management policies which, for instance, include administrator access to operating systems as well as databases.

b. Third parties involved in either cloud computing and/or data offshoring arrangements should develop and implement adequate user access privilege controls in order to restrict access to the bank's data, systems and infrastructure. This should be done in a granular fashion and on a least-privilege basis. It remains the responsibility of the bank to ensure that these controls are in place and are operating efficiently.

c. The bank remains responsible for ensuring that processes for user provisioning (on-boarding), deprovisioning (termination) and job function changes are managed in a timely and controlled manner in line with its user access policies.

4.7.8 Encryption

a. Banks should determine the level of encryption required in line with the classification of the data involved in the cloud computing or data offshoring arrangement. With cloud computing, the deployment model followed is also of relevance in determining the appropriate level of encryption. All subsequent encryption considerations should be read in line with the principle that the level of encryption should be commensurate with the materiality of the data and risks involved.

b. Banks would use different classifications, but for any personal, private or confidential data in a multitenant and/or community/public cloud environment, banks should consider encrypting data in transit as well as in storage.
c. Where encryption is required, data should be encrypted before it is moved to the cloud and/or offshored, and the same level of encryption services should be used for data at rest and in motion.
d. Access to encryption keys should be restricted in line with the bank's key management policies and procedures. Where third parties are involved, key management should be subject to the same level of control as outlined in the bank's policies and procedures.
e. Policies and procedures should cover public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, recoverability, exchange and storage, where applicable.
f. Where third parties are used, they should inform the bank of changes within their cryptosystems.

4.7.9 Incident management

a. The contractual agreement with any third party involved in cloud computing and data offshoring should refer to the incident management process between the parties, and set out the roles and responsibilities of the respective parties.
b. The incident management process should include incident notifications, responses, remediation, documentation, timelines, addressing the risk of the incident, escalation, and formally closing incidents.
c. The contractual agreement with the third party should define the types of incidents (for instance data breaches and security violations), events and the actions to be initiated after each incident.
d. Banks should be informed when their data may have been seized or accessed by a foreign country, even if it is through appropriate legal processes in that country.

4.7.10 Multitenancy in the cloud

a. It is the responsibility of the bank to ensure that the security requirements of the bank are commensurate with its risk appetite. The bank should take reasonable steps to ensure that its data in its possession is sufficiently protected, irrespective of whether it is hosted in the cloud.
b. As part of defining and agreeing on security standards, the security configuration baseline to prevent cross-contamination with other customer environments should be considered.

4.7.11 Virtualised environments

a. Banks should be aware of the types of virtualisation used by third-party service providers and assess whether the level of security within the third party's environment is adequate or whether it should be augmented by additional security technologies.

b. As part of defining and agreeing on security standards, the security configuration baseline to harden virtualised operating systems should be defined, where applicable.
c. The agreed security standards should further address hypervisor vulnerability management, patch management and release management – specifically when new vulnerabilities are discovered.

4.8 Guidelines for compliance with paragraph 2.2.8 of Directive 3/2018 requiring that 'banks that use cloud computing and/or offshoring of data must ensure that they remain compliant with applicable legislation and regulations, both local as well as in any country where the cloud services and/or data are hosted'.

4.8.1 Accountability

a. Banks retain accountability for compliance with all legislative requirements and should therefore ensure that a contractual agreement with third parties incorporates the necessary arrangements that will enable them to remain compliant.
b. It further remains the bank's responsibility to evidence compliance.
c. Refer to paragraphs 6.1.2 and 6.4.2 of G5/2014 for additional guidance on accountability for outsourcing arrangements surrounding board accountability and the consideration of compliance requirements during due diligence processes.

4.8.2 Compliance landscape

a. Banks should take all their respective regulators into consideration when considering cloud computing and/or data offshoring arrangements in order to ensure compliance. Banks should be aware that, apart from local legislative requirements, regulators in other jurisdictions may impose additional requirements on the bank.
b. Banks should be aware of the legislative requirements applicable to the third party in the countries where the bank's data is hosted and determine whether this does not impose undue risk on the bank, especially where countries have rights to seize or otherwise access data hosted by the third party.
c. The regulatory and compliance landscape should be monitored for changes and the bank's compliance framework should be regularly updated.

4.8.3 Compliance in contracts

a. The terms of contractual agreement should allow a bank to modify the manner in which the cloud computing and/or data offshoring activities are performed, specifically where banks may need to amend processes to meet compliance requirements.
b. Where a bank makes use of a third party in the use of cloud computing and/or data offshoring, the bank should ensure that it contractually agrees on the compliance requirements with the service provider to ensure ongoing compliance with laws and regulations where the data shall be hosted.

4.9 Guidelines for compliance with paragraph 2.2.9 of Directive 3/2018 requiring that 'the use of cloud computing and/or offshoring of data must not in any way infringe on the bank's supervisors and prevent any regulatory mandated access to information nor must it impact on its regulators' ability to fulfil their duties'.

4.9.1 Contractual arrangements must be in place to ensure access to data by all relevant parties, including the bank's regulatory authorities such as the relevant departments of the SARB, the Financial Sector Conduct Authority (FSCA) and the FIC.

4.9.2 Ability to regulate and access to data:

a. The contractual agreement should include the right of supervisory institutions to access information, which includes conducting on-site visits at the service provider's facilities, where considered necessary.
b. Should the senior management of a bank become aware of any possible restriction on the access to regulatory data, the PA has to be informed thereof, as soon as practically possible.
c. The contractual agreement should provide for the mutual exchange of information (potentially through a right to transparency clause) and, by request, the provision of relevant information to the bank's supervisors. Where a bank is unable to present data to its supervisor upon request, for any reason whatsoever, the PA may request the termination of the relationship with the service provider and take further steps as deemed necessary.
d. Banks should ensure that data is not stored in jurisdictions that may inhibit effective access to data for South African supervisors. In considering jurisdictions, banks should continually take into account the political and security stability of the jurisdiction as well as the legislative requirements of the jurisdiction in question. This should include consideration of the legal enforcement provisions within a jurisdiction.

4.9.3 Right to audit

a. The contractual agreement with the third party should contain a right to audit clause which is clearly defined and satisfies the assurance requirements of the bank's board, audit charter, external auditors and any regulators that have jurisdiction over the bank.
b. The right to audit clause is listed for inclusion in outsourcing contracts in paragraph 6.5.2 of G5/2014.

4.10 Guidelines for compliance with paragraph 2.2.10 of Directive 3/2018 requiring that 'banks must have contingency plans in place to continue operations, meet their core obligations, i.e. regulatory, statutory or otherwise, despite any cloud computing or offshoring arrangements which may be in place'.

4.10.1 Capacity

a. Before entering into a contract with a third party, banks should assess whether the third party has sufficient capacity to effectively manage, on a continuous basis, the services that the bank is planning to move to the cloud and/or offshore. Banks should also consider the potential increased services that the third party may have to provide in the foreseeable future, including the relevant metrics for capacity, such as storage capacity, bandwidth requirements, increased number of users, and transactions per second requirements.
b. Before entering into any third-party contracts, banks should consider whether the information communications infrastructure between the bank and the third party is sufficient to manage the current and future requirements on a continual basis.

4.10.2 Continuity and recoverability

a. Refer to paragraph 6.7 of G5/2014 for additional guidance on contingency planning and continuity for outsourcing arrangements.
b. Banks should be able to recover from any failure of a third party within a reasonable time frame, as well as within legal and regulatory imposed timelines.
c. Business continuity requirements, such as recovery time and recovery point objectives (RTOs and RPOs), should be identified through a business impact assessment, documented and, where third parties are involved, agreed with third parties.
d. Disaster recovery and business continuity plans should be developed to maintain continuity of the bank's operations, including matters related to the recovery from an incident, plans for communicating incidents, and the frequency of testing the adequacy and effectiveness of these plans.
e. Resilience should be designed/built into the bank's cloud computing and/or data offshoring arrangements.
f. Before contracting with any third party, a bank should consider whether the third party's business continuity measures are commensurate with the bank's requirements.
g. Banks should have access to the audit or assurance reports of the third party's business continuity programme, including disaster recovery testing, process audits and control audits at least for activities/functions managed on their behalf.
h. The third party's business continuity programme should ideally be certified or mapped to internationally recognised standards such as ISO 22301 (business continuity management systems).
i. The roles and responsibilities of the bank and any third party in the event of a disruption should be clearly defined in the contractual arrangements.
j. Banks retain overall responsibility to ensure the availability of their data and services to persons/entities that may legally access such data and services.
k. Contingency plans pertaining to outsourced activities should be reviewed regularly, but not less frequently than once a year.

4.11 Guidelines for compliance with paragraph 2.2.11 of Directive 3/2018 requiring that 'banks must ensure that their intellectual property rights and contractual rights to data are not compromised, despite any cloud computing or data offshoring arrangements which may be in place. Data must always be in a usable, readable and portable state even when the contract is terminated'.

4.11.1 Planning for termination

a. Banks should document the hardware, software and procedural requirements for moving from an existing service provider to another service provider or in-house. As far as it is feasibly possible, a bank should avoid being locked into one specific service provider.
b. Banks need to ensure that an exit from a cloud computing and/or offshoring of data arrangement does not affect their compliance with any legislative requirements.

4.11.2 Contractual agreements

a. According to paragraph 6.5.2 of G5/2014, default and termination provisions should be included in outsourcing contracts.
b. The contractual agreement should stipulate the roles and responsibilities for both parties at the termination of the agreement, including the circumstances when a bank enters into a SARB resolution.
c. The contractual agreement should define the manner in which the agreement is to be terminated as well as the guarantees provided to enable the bank to resume performance of the outsourced and/or offshored activities or to transfer those activities to another service provider upon termination of the agreement.
d. The contractual agreement should include a clause to the effect that, upon the termination of the contract, a bank's data be promptly and completely removed and returned to the bank, transferred to another service provider or destroyed, depending on the nature of the data involved. The contractual arrangements should include sufficient assurance once its data has been removed, transferred or destroyed at the termination of the agreement.

4.11.3 Termination of services

a. Any cloud computing and/or data offshoring services should be organised in such a way that they do not become a barrier to the resolution or orderly wind-down of a bank, or create additional complexity in a resolution.
b. Where functions and/or data outsourced or offshored are identified in a bank's recovery plan, banks should provide further detail and guidance in the recovery plan on the cloud computing and/or offshoring involved, such as the effect recovery would have on the relationship, as well as actions required to ensure continuity during recovery of the bank or failure of the service provider.

c. The contractual agreement for a cloud computing and/or data offshoring arrangement, specifically any default clause, may not entitle the service provider to unilaterally cancel the agreement in the event that a recovery or resolution action is taken.

4.11.4 Interoperability

a. Banks should consider interoperability before outsourcing activities to a CSP or data offshoring.
b. As part of its business continuity planning and testing, a bank should maintain as well as test procedures, capabilities and alternatives to transfer cloud computing and/or offshored data and operations in-house or to another third party as part of a scenario where the current third party service provider is no longer able to meet its contractual obligations.
c. The bank should have contingency plans in place to continue with its operations in case of an unforeseen event, irrespective of whether a cloud environment had been deployed. The bank's risk management processes should determine the level and extent of contingency plans to be instituted. The operational requirements can be addressed on a case-by-case basis given the existing circumstances.

4.12 Guidelines for compliance with paragraph 2.2.12 of Directive 3/2018 requiring that 'any cloud computing and/or offshoring of data arrangements must not impact on a bank's ability to conduct forensic audits or investigations'.

4.12.1 Applicability

a. Forensic measures for public data hosted on a public cloud should be commensurate with the bank's risk appetite. It is expected that the control measures in the cloud and offshored environments should be commensurate with the internal controls of the bank and that sensitive data should not be subjected to less stringent control measures in a cloud or offshored environment.
b. Data produced for regulatory reporting purposes should be reconcilable with source data and banks should be able to prove that the integrity of such data has been preserved, which includes data reported to all regulatory authorities.

4.12.2 Contractual agreements

a. The contractual agreement with the third parties responsible for cloud computing and/or the offshoring of data must clearly prescribe the access that the bank, regulatory authorities and law enforcement agencies would have in order to conduct forensic audits and investigations.
b. The contractual agreement should prescribe the manner in which forensic evidence is made available to the bank as well as the controls in place as proof that such evidence has not been tampered with.
c. The contractual agreement should define the roles and responsibilities for both parties in terms of forensic data. This should, for instance, include who is responsible for logging which data.

d. The contractual agreement should also determine which forensic tools are available to a bank directly or via the third party.
e. The contractual agreement should further stipulate both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony. A bank should be able to provide adequate assurance to investigative and regulatory authorities that all data requested has been retrieved.
f. The contractual agreement should stipulate the duration during which forensic data would be available to a bank.
g. The contractual agreement with the third party should require assurance that the bank's data is preserved as recorded, which includes both the primary data and secondary information, such as metadata and logs.

4.12.3 Planning for forensics

a. Where forensic evidence is not available to the bank, it should consider whether the risk is justified for each cloud initiative, particularly considering the sensitivity of data involved and compliance requirements.
b. Banks should consider the availability of data and records if required for forensic audits which may, specifically in a multitenant environment, be commingled and migrated among multiple servers located across national boundaries, which may make it impossible to identify specific data.
c. A bank should consider that where a court or government grants access to a third party's servers, such local authorities might have access to the bank's forensic data. This should ideally not include a bank's customer data, which should be encrypted, with the bank restricting access to the encryption keys.

4.13 Guidelines for compliance with paragraph 2.2.13 of Directive 3/2018 requiring that 'all cloud computing and/or data offshoring arrangements must be contained in a documented, legally binding agreement'.

4.13.1 Contractual agreements

a. The importance of a comprehensive contractual agreement, including SLAs, cannot be overemphasised.
b. The contract and SLAs should be reviewed by the bank's legal counsel before being signed, and the cloud computing and/or data offshoring relationship should not start before the contract has been signed by all parties.
c. The contractual agreement with the third parties involved in cloud computing and/or data offshoring should define the third party's contractual obligations as guardian of a bank's data.
d. Banks should ensure that the contractual agreement provides all elements relevant to the cloud computing and/data offshoring arrangement, including sufficient protection of data applicable to the nature of services being offered, deployment of services structurally and geographically, and compliance with the laws in the various jurisdictions where the data will be hosted or stored.

e. Refer to paragraph 6.5 of G5/2014 for additional guidance on outsourcing contracts.

4.13.2 Data ownership

a. The contractual agreement with any third party involved in cloud computing and/or data offshoring arrangements should clearly state that the bank retains ownership rights of the data.
b. Both the bank and the third party should understand how the data ownership rights are affected by the different laws of the countries which will host the data.

4.13.3 Banks should obtain assurance from the service provider of cloud computing and/or the offshoring of data that data, including all copies and backups, are stored only in geographic locations permitted by the contractual agreements in line with the bank's regulatory and legislative requirements.

4.13.4 The contractual agreement should clearly state which activities may be subcontracted by a third party and that such arrangements would be subject to full compliance with the primary contractual agreement, including meeting all regulatory and compliance requirements stipulated therein. The primary contract should clearly state that the service provider remains liable for performance in terms of the contract despite any subcontracting arrangements.

4.13.5 The service provider shall provide an undertaking to treat the bank's data with the utmost confidentiality at all times and to ensure that its employees and service providers adhere to the same standard of confidentiality. Access should be restricted on a least-privilege basis.

4.13.6 Data breaches

a. The bank is responsible for ensuring that the contractual agreement with the service provider ensures that it is able to meet its data breach notification or other legal reporting requirements.
b. The contractual agreement should define roles and responsibilities in case of a data breach, including cooperative processes to be implemented during the investigation and any follow-up actions.
c. The contractual agreement should define the penalties payable by the third party for data breaches where the third party did not adhere to the terms of the agreement or was negligent in any other way.

4.13.7 The use of cloud computing or the offshoring of data should not inhibit the bank's ability to meet its data retention legal requirement.

4.13.8 All legal documents should be maintained in accordance with the bank's legal document management procedures and in accordance with legislative requirements.

5. Acknowledgement of receipt

5.1 Kindly ensure that a copy of this guidance note is made available to your institution's external 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 guidance note issued was Guidance Note 4/2018, dated 5 September 2018.