South African Reserve Bank

Financial Surveillance Department

2020-10-01

Exchange Control Circular No. 10/2020

Offshoring and cloud computing

Authorised Dealers and Authorised Dealers in foreign exchange with limited authority are advised that during June 2019 a position paper outlining the views of the Financial Surveillance Department with regard to offshoring and cloud computing by Authorised Dealers and reporting entities was published for comments.

Based on the responses, some common themes were identified and the proposed policy document was updated to simplify the requirements and to provide more clarity on the fact that the position paper is only applicable to functions, services, business processes, data, infrastructure and systems of reporting entities as contemplated in terms of the Currency and Exchanges Manual for Authorised Dealers and Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority. See Annexure A for the signed copy of the 'Offshoring and cloud computing position paper'.

Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to the Financial Surveillance Department. In addition to ensuring compliance with the requirements and assurances specified by the Financial Surveillance Department, reporting entities must also be in compliance with the requirements of all other regulatory and supervisory institutions as well as applicable legislation. Specific reference is made to the directive (D3/2018) and guidance notes (G5/2018) with regard to offshoring and cloud computing issued by the Prudential Authority of the South African Reserve Bank.

The ultimate responsibility for ensuring that the risks associated with offshoring and cloud computing are duly managed, vests with the relevant reporting entities. Failure to comply with any of the requirements outlined by the Financial Surveillance

Department may result in measures being taken by it as administrator of the exchange control system.

The following amendments have been made to the Currency and Exchanges Manual for Authorised Dealers:

A new subsection J.(D) has been inserted and the current sections J.(D) to J.(H) have been renumbered J.(E) to J.(I) respectively:

(D) Offshoring and cloud computing

(i) The Financial Surveillance Department is prepared to consider requests to authorise the following offshoring and cloud computing models relevant exclusively to data, infrastructure and systems, as contemplated in the Authorised Dealer Manual:

(a) offshoring within a reporting entity's international head office and/or group;

(b) cloud computing relating to data, infrastructure and systems;

(c) local outsourcing of data, infrastructure and systems; and

(d) real-time system and data replication to South Africa from an international head office and/or group.

(ii) The Financial Surveillance Department is not agreeable to the following offshoring and cloud computing models:

(a) offshoring, local and international outsourcing or cloud computing of functions, services and business processes as contemplated in the Authorised Dealer Manual; and

(b) any form of offshoring and cloud computing models where data is stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(iii) Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to the Financial Surveillance Department.

(iv) The following requirements must be adhered to:

(a) Agreements

(aa) A documented legally binding agreements or contracts must be concluded with the reporting entity's Head Office or any other third party that forms part of the proposed operating model. These agreements or contracts must state, but not be limited to, the following:

(1) data relevant to the reporting entity will be ring-fenced from other activities of the data centre to be used and should stipulate how it will be achieved;

(2) data will be retained for a minimum period of five years, as required by the Authorised Dealer Manual; and

(3) data will be accessible immediately, but not later than 48 hours, from the source systems and extractable in the format prescribed in (h)(gg) below.

(bb) Any amendments to the above agreements/contracts with regard to a change in the approved operating model requires prior approval of the Financial Surveillance Department.

(b) Risk assessment

(aa) Prior to undertaking a particular offshoring and cloud computing initiative, a reporting entity must perform a risk assessment, which must be documented.

(bb) The risk assessment must identify all risks involved and determine whether adequate controls can be implemented to mitigate any potential risks.

(cc) A reporting entity must have documented processes and procedures in place to, on a continuous basis identify, assess, manage and mitigate risks associated with offshoring and cloud computing.

(dd) Risks must be adequately understood and managed prior to entering into an offshoring and cloud computing arrangement. Factors that must be addressed include, inter alia, continuity, data protection, regulatory access to data and regulatory compliance.

(c) Business continuity plan

(aa) A reporting entity must satisfy itself that the data centre hosting the data must have extensive disaster recovery and business continuity processes and procedures in place.

(bb) Regular disaster recovery tests must be performed to ensure data can be recovered.

(d) Storage of data

(aa) All data must be ring-fenced without the ability to be updated by unauthorised persons.

(bb) Cross-border transactional data must be stored directly into the source system, i.e. the core accounting system.

(cc) Customer data must be stored directly from the source system, i.e. the centralised customer database.

(dd) In an event of the reporting entity terminating its operations in South Africa for any reason whatsoever, data for five years preceding the date of termination, must be replicated to South Africa by the reporting entity in a format accessible by the Financial Surveillance Department and within an agreed period.

(e) Regulatory access to data

(aa) Any data required by the Financial Surveillance Department must be made available for access immediately, but not later than 48 hours, by the reporting entity and should forthwith be furnished to the Financial Surveillance Department in the format prescribed in paragraph (h)(gg) below.

(bb) Information must be made available, upon request, at no cost to the Financial Surveillance Department.

(cc) The use of offshoring and cloud computing may not in any way infringe on the Financial Surveillance Department's mandated access to data.

(f) Jurisdiction

(aa) A reporting entity must ensure that data is not stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(bb) In considering foreign jurisdictions, a reporting entity must take into account the wider political and security stability of the particular jurisdiction as well as the legislative requirements in terms of the foreign jurisdiction concerned. This should include consideration of the legal enforcement provisions within a jurisdiction.

(g) Procedure to update data back to source

(aa) From time to time a reporting entity may be required to amend certain data, e.g. balance of payments categories or cancel the reporting of a transaction. This might have an impact on the same source reporting principle, as all changes must be updated back to the source, i.e. transactional or accounting system.

(h) System requirements

(aa) Data in any offshore data centre must at the least be encrypted through modern encryption technology.

(bb) All cryptographic keys used in a storage encryption solution must be secured and managed properly to support the security of the solution.

(cc) To prevent the non-recovery of encrypted data, extensive planning of key management processes, procedures, and technologies should be performed before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery and destruction.

(dd) Only authorised personnel and systems must be able to retrieve, decrypt and process data through any network or cloud.

(ee) The foreign service provider should have very strong, documented and tested cyber controls to protect data against cybercrime.

(ff) A reporting entity must verify adherence to the agreed information security requirements, i.e. through third party assurance audits and/or any other security testing

requirements such as vulnerability scanning and penetration testing.

(gg) Data requested by the Financial Surveillance Department should be provided in a standard report format, as prescribed in the Authorised Dealer Manual, such as a semi-colon delimited file (e.g.CSV).

(i) Other regulatory bodies and legislative requirements

(aa) A reporting entity must consider the offshoring and cloud computing models in the context of its overarching regulatory obligations, which may include obligations to the Financial Intelligence Centre and the Prudential Authority who have different statutory objectives and may, therefore, have different requirements.

(bb) A reporting entity must acquaint itself with the relevant provisions of the applicable legislation, e.g. the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) and Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001).

(v) Applications to the Financial Surveillance Department should, inter alia, include the following:

(a) confirmation that the reporting entity complies with the requirements and assurance set out in (iii) above and (v) below; and

(b) a copy of the business case which should outline, inter alia, the following:

(aa) proposed offshoring and cloud computing operating model;

(bb) details of all relevant offshoring and cloud computing third parties or service providers;

(cc) benefits and risks involved;

(dd) confirmation that the management and mitigation of risks is done in order to maximise the benefits through effective end-to-end governance practices;

(ee) jurisdictions where data will be stored;

(ff) service, deployment and security models of offshoring and cloud computing applicable to the different classifications of data;

(gg) how data loss and breaches will be dealt with;

(hh) procedure to ensure that the reporting requirements stated in the Authorised Dealer Manual are adhered to;

(ii) procedures to be implemented to accommodate requests to update data from the source systems; and

(jj) strategy to be implemented in the event that offshoring and cloud computing operations are required to be moved from one provider to another.

(vi) Assurances

(a) The compliance with all the requirements listed in (iii) above, must be contained in the Managerial Letter of Comfort to be provided to the Financial Surveillance Department on an annual basis.

(vii) Remedies

(a) Any failure by a reporting entity to comply with the above mentioned requirements may result in the suspension of authorities provided by the Financial Surveillance Department or may cause the

Financial Surveillance Department to invoke remedies available to it in terms of the Exchange Control Regulations.

The following amendments have been made to the Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority:

A new subsection C.1(D) has been inserted and the current sections C.1(D) to C.1(H) have been renumbered C.1(E) to C.1(I) respectively:

(D) Offshoring and cloud computing

(i) The Financial Surveillance Department is prepared to consider requests to authorise the following offshoring and cloud computing models relevant exclusively to data, infrastructure and systems, as contemplated in the ADLA Manual:

(a) offshoring within a ADLA's international head office and/or group;

(b) cloud computing relating to data, infrastructure and systems;

(c) local outsourcing of data, infrastructure and systems; and

(d) real-time system and data replication to South Africa from an international head office and/or group.

(ii) The Financial Surveillance Department is not agreeable to the following offshoring and cloud computing models:

(a) offshoring, local and international outsourcing or cloud computing of functions, services and business processes as contemplated in the ADLA Manual; and

(b) any form of offshoring and cloud computing models where data is stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(iii) Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to the Financial Surveillance Department.

(iv) The following requirements must be adhered to:

(a) Agreements

(aa) A documented legally binding agreements or contracts must be concluded with the ADLA's Head Office or any other third party that forms part of the proposed operating model. These agreements or contracts must state, but not be limited to, the following:

(1) data relevant to the ADLA will be ring-fenced from other activities of the data centre to be used and should stipulate how it will be achieved;

(2) data will be retained for a minimum period of five years, as required by the ADLA Manual; and

(3) data will be accessible immediately, but not later than 48 hours, from the source systems and extractable in the format prescribed in (h)(gg) below.

(bb) Any amendments to the above agreements/contracts with regard to a change in the approved operating model requires prior approval of the Financial Surveillance Department.

(b) Risk assessment

(aa) Prior to undertaking a particular offshoring and cloud computing initiative, an ADLA must perform a risk assessment, which must be documented.

(bb) The risk assessment must identify all risks involved and

determine whether adequate controls can be implemented to mitigate any potential risks.

(cc) An ADLA must have documented processes and procedures in place to, on a continuous basis identify, assess, manage and mitigate risks associated with offshoring and cloud computing.

(dd) Risks must be adequately understood and managed prior to entering into an offshoring and cloud computing arrangement. Factors that must be addressed include, inter alia, continuity, data protection, regulatory access to data and regulatory compliance.

(c) Business continuity plan

(aa) An ADLA must satisfy itself that the data centre hosting the data must have extensive disaster recovery and business continuity processes and procedures in place.

(bb) Regular disaster recovery tests must be performed to ensure data can be recovered.

(d) Storage of data

(aa) All data must be ring-fenced without the ability to be updated by unauthorised persons.

(bb) Cross-border transactional data must be stored directly into the source system, i.e. the core accounting system.

(cc) Customer data must be stored directly from the source system, i.e. the centralised customer database.

(dd) In an event of the ADLA terminating its operations in South Africa for any reason whatsoever, data for five years

preceding the date of termination, must be replicated to South Africa by the ADLA in a format accessible by the Financial Surveillance Department and within an agreed period.

(e) Regulatory access to data

(aa) Any data required by the Financial Surveillance Department must be made available for access immediately, but not later than 48 hours, by the ADLA and should forthwith be furnished to the Financial Surveillance Department in the format prescribed in paragraph (h)(gg) below.

(bb) Information must be made available, upon request, at no cost to the Financial Surveillance Department.

(cc) The use of offshoring and cloud computing may not in any way infringe on the Financial Surveillance Department's mandated access to data.

(f) Jurisdiction

(aa) An ADLA must ensure that data is not stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(bb) In considering foreign jurisdictions, an ADLA must take into account the wider political and security stability of the particular jurisdiction as well as the legislative requirements in terms of the foreign jurisdiction concerned. This should include consideration of the legal enforcement provisions within a jurisdiction.

(g) Procedure to update data back to source

(aa) From time to time an ADLA may be required to amend certain data, e.g. balance of payments categories or cancel

the reporting of a transaction. This might have an impact on the same source reporting principle, as all changes must be updated back to the source, i.e. transactional or accounting system.

(h) System requirements

(aa) Data in any offshore data centre must at the least be encrypted through modern encryption technology.

(bb) All cryptographic keys used in a storage encryption solution must be secured and managed properly to support the security of the solution.

(cc) To prevent the non-recovery of encrypted data, extensive planning of key management processes, procedures, and technologies should be performed before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery and destruction.

(dd) Only authorised personnel and systems must be able to retrieve, decrypt and process data through any network or cloud.

(ee) The foreign service provider should have very strong, documented and tested cyber controls to protect data against cybercrime.

(ff) An ADLA must verify adherence to the agreed information security requirements, i.e. through third party assurance audits and/or any other security testing requirements such as vulnerability scanning and penetration testing.

(gg) Data requested by the Financial Surveillance Department should be provided in a standard report format, as prescribed

in the ADLA Manual, such as a semi-colon delimited file (e.g.CSV).

(i) Other regulatory bodies and legislative requirements

(aa) An ADLA must consider the offshoring and cloud computing models in the context of its overarching regulatory obligations, which may include obligations to the Financial Intelligence Centre and the Prudential Authority who have different statutory objectives and may, therefore, have different requirements.

(bb) An ADLA must acquaint itself with the relevant provisions of the applicable legislation, e.g. the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) and the FIC Act.

(v) Applications to the Financial Surveillance Department should, inter alia, include the following:

(a) confirmation that the ADLA complies with the requirements and assurance set out in (iv) above and (vi) below; and

(b) a copy of the business case which should outline, inter alia, the following:

(aa) proposed offshoring and cloud computing operating model;

(bb) details of all relevant offshoring and cloud computing third parties or service providers;

(cc) benefits and risks involved;

(dd) confirmation that the management and mitigation of risks is done in order to maximise the benefits through effective end-to-end governance practices;

(ee) jurisdictions where data will be stored;

(ff) service, deployment and security models of offshoring and cloud computing applicable to the different classifications of data;

(gg) how data loss and breaches will be dealt with;

(hh) procedure to ensure that the reporting requirements stated in the ADLA Manual are adhered to;

(ii) procedures to be implemented to accommodate requests to update data from the source systems; and

(jj) strategy to be implemented in the event that offshoring and cloud computing operations are required to be moved from one provider to another.

(vi) Assurances

(a) The compliance with all the requirements listed in (iv) above, must be contained in the Managerial Letter of Comfort to be provided to the Financial Surveillance Department on an annual basis.

(vii) Remedies

(a) Any failure by an ADLA to comply with the above mentioned requirements may result in the suspension of authorities provided by the Financial Surveillance Department or may cause the Financial Surveillance Department to invoke remedies available to it in terms of the Exchange Control Regulations.

The amended Currency and Exchanges Manual for Authorised Dealers and the Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority may be accessed on the SARB website: www.resbank.co.za by

following the links: Home>Regulation and supervision>Financial surveillance and exchange controls>Currency and exchanges documents.

Head of Department: Financial Surveillance

Annexure A

South African Reserve Bank

Financial Surveillance Department

Offshoring and cloud computing position paper

August 2020

Contents

1. Executive summary

1.1 The purpose of this position paper is to outline the Financial Surveillance Department (FinSurv) of the South African Reserve Bank's (SARB) view with regard to offshoring and cloud computing by Authorised Dealers, Authorised Dealers in foreign exchange with limited authority and direct reporting entities (hereafter referred to as a reporting entity(ies)).

1.2 Although FinSurv acknowledges the possible benefits and is not necessarily averse to the concept of offshoring and cloud computing, certain requirements and assurances by reporting entities will have to be adhered to, to ensure, inter alia, the confidentiality, integrity and availability of data.

1.3 Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to FinSurv. In addition to ensuring compliance with the requirements and assurances specified by FinSurv, reporting entities must also be in compliance with the requirements of all other regulatory and supervisory institutions as well as applicable legislation. Specific reference is made to the directive (D3/2018) and guidance notes (G5/2018) with regard to offshoring and cloud computing issued by the Prudential Authority of SARB.

1.4 The ultimate responsibility for ensuring that the risks associated with offshoring and cloud computing are duly managed, vests with the relevant reporting entities. Failure to comply with any of the requirements outlined by FinSurv may result in measures being taken by FinSurv as administrator of the exchange control system.

2. Introduction

2.1 Purpose of this position paper

2.1.1 This position paper sets out FinSurv's view insofar as offshoring and cloud computing may affect the application of exchange controls.

2.1.2 The Minister of Finance has delegated all the powers and functions conferred and all duties assigned to and imposed on the National Treasury under the Exchange Control Regulations (with certain exceptions), to the Governor and/or a Deputy Governor, as well as to the Head of FinSurv (and to other officials in FinSurv). This delegation, in essence, renders FinSurv responsible for the day-to-day administration of exchange controls in South Africa.

2.1.3 As part of this administration, FinSurv, inter alia, collects and maintains information which is more sensitive than aggregated information collected by other departments within SARB. This includes, but is not limited to, cross-border transactional data, customer information and digital images of documentation, e.g. documentary evidence obtained in terms of the Currency and Exchanges Manual for Authorised Dealers (Authorised Dealer Manual) and the Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority (ADLA Manual), (hereafter collectively referred to as data).

2.1.4 The purpose of this position paper, therefore, outlines FinSurv's view of utilising both offshoring as well as cloud computing by reporting entities. It also sets out key requirements and conditions that should be met when engaging in these activities. The requirements and conditions will, however, vary depending on the model of offshoring and cloud computing implemented by the reporting entities.

2.2 Regulatory concern

2.2.1 Since FinSurv is responsible for the day-to-day administration of exchange controls in South Africa by virtue of the delegation by the Minister of Finance, it requires assurance that data remains confidential, accurate and readily available in order to fulfil its mandate and to avoid its duties being compromised.

2.2.2 Currently, the Exchange Control Regulations and FinSurv reporting standards as outlined in the Authorised Dealer Manual and the ADLA Manual do not make provision for offshoring and cloud computing. However, FinSurv identified a need to review its current position on offshoring and cloud computing.

2.2.3 FinSurv requires assurance that compliance with South African legislative requirements are considered and adhered to by the reporting entities.

3. Key concepts

3.1 Description of key concepts

3.1.1 For the purpose of this FinSurv position paper, the following key concepts are outlined below:

Concept	Description
Business processes	Business processes refer to FinSurv related business processes which include, but are not limited to, on-boarding of customers, exchange control compliance, sanction screenings, releasing of cross-border payments and activities relating to reporting to FinSurv.
Data	Data refers to cross-border transactional data, customer information and digital images of documentation, e.g. documentary evidence obtained in terms of the Authorised Dealer Manual and ADLA Manual.
Customer information	Customer information is data captured in the centralised customer database of reporting entities which, inter alia, includes data captured during on-boarding of a customer, client identification and verification documentation as obtained in terms of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001).
Transactional data	Transactional data is cross-border transactional data reported by reporting entities to FinSurv in terms of the provisions outlined in the Authorised Dealer Manual and ADLA Manual.

Concept	Description
Digital images of documentation	Digital images of documentation includes documentary evidence obtained and/or stored in an electronic format by reporting entities as outlined in the Authorised Dealer Manual, ADLA Manual or specified in terms of certain approvals granted by FinSurv.
Offshoring	Offshoring is the transferring of the business processes (including, but not limited to exchange control compliance), services, systems, data or infrastructure of the reporting entities to a branch or Head Office situated outside the borders of South Africa.
Cloud computing	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. Forms of cloud computing may include a public cloud, private cloud, community cloud or hybrid cloud. Computers providing capacity can be in different geographical locations which may be subject to different laws, business practices and government oversight.
Local outsourcing	Local outsourcing is the subcontracting of business processes (including, but not limited to exchange control compliance), functions, services, systems, data or infrastructure of reporting entities, as contemplated in the Authorised Dealer Manual and ADLA Manual, to a third party within South African jurisdiction but not based at the premises of the relevant reporting entities.
International outsourcing	International outsourcing is the subcontracting of business processes (including, but not limited to exchange control compliance), functions, services, systems, data or infrastructure

Concept	Description
	of reporting entities, as contemplated in the Authorised Dealer Manual and ADLA Manual to a third party situated outside the borders of South Africa.
Regulatory access to data	Regulatory access to data refers to FinSurv's access to data and systems. This includes access to transactional systems' front-end and back-end systems as well as folders, servers and databases.
System replication	System replication refers to duplication of transactional systems' front-end and back-end systems as well as folders, servers and databases. This also includes the replication tools used to keep transactional systems' front-end and back-end systems as well as folders, servers and databases synchronised.
Data replication	Data replication refers to the process of copying data from one location to another, including the replication tools used.

4. The position of the Financial Surveillance Department on offshoring and cloud computing

4.1 FinSurv recognises that there is a growing demand to utilise offshoring and cloud computing. FinSurv's preference remains to have all FinSurv related functions, services, business processes, data, infrastructure and systems of reporting entities within South Africa.

4.2 FinSurv, however, is prepared to consider requests to authorise the following offshoring and cloud computing models relevant exclusively to data, infrastructure and systems, as contemplated in the Authorised Dealer Manual and ADLA Manual:

(i) offshoring within a reporting entity's international head office and/or group;

(ii) cloud computing relating to data, infrastructure and systems;

(iii) local outsourcing of data, infrastructure and systems; and

(iv) real-time system and data replication to South Africa from an international head office and/or group.

4.3 FinSurv is not agreeable to the following offshoring and cloud computing models:

(i) offshoring, local and international outsourcing or cloud computing of functions, services and business processes as contemplated in the Authorised Dealer Manual and ADLA Manual; and

(ii) any form of offshoring and cloud computing models where data is stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

5. Application procedure

5.1 All requests for offshoring and cloud computing by a reporting entity must be submitted in the form of a formal application to FinSurv for consideration.

5.2 The application must provide:

5.1.1 confirmation that the reporting entity complies with the requirements and assurance set out in paragraphs 6 and 7 below; and

5.1.2 a copy of the business case which should outline, inter alia, the following:

(i) proposed offshoring and cloud computing operating model;

(ii) details of all relevant offshoring and cloud computing third parties or service providers;

(iii) benefits and risks involved;

(iv) confirmation that the management and mitigation of risks is done in order to maximise the benefits through effective end-to-end governance practices;

(v) jurisdictions where data will be stored;

(vi) service, deployment and security models of offshoring and cloud computing applicable to the different classifications of data;

(vii) how data loss and breaches will be dealt with;

(viii) procedure to ensure that the FinSurv reporting requirements stated in the Authorised Dealer Manual, the ADLA Manual and this position paper are adhered to;

(ix) procedures to be implemented to accommodate requests to update data from the source systems; and

(x) strategy to be implemented in the event that offshoring and cloud computing operations are required to be moved from one provider to another.

6. Requirements

6.1 Agreements

6.1.1 A reporting entity must conclude documented legally binding agreements or contracts with its Head Office or any other third party that forms part of the proposed operating model. These agreements or contracts must state, but not be limited to, the following:

(i) data relevant to the reporting entity will be ring-fenced from other activities of the data centre to be used and should stipulate how it will be achieved;

(ii) data will be retained for a minimum period of five years, as required by the Authorised Dealer Manual and ADLA Manual; and

(iii) data will be accessible immediately, but not later than 48 hours, from the source systems and extractable in the format prescribed in paragraph 6.8.7 below.

6.1.2 Any amendments to the above agreements/contracts with regard to a change in the approved operating model requires prior approval of Finsurv.

6.2 Risk assessment

6.2.1 Prior to undertaking a particular offshoring and cloud computing initiative, a reporting entity must perform a risk assessment, which must be documented.

6.2.2 The risk assessment must identify all risks involved and determine whether adequate controls can be implemented to mitigate any potential risks.

6.2.3 A reporting entity must have documented processes and procedures in place to, on a continuous basis identify, assess, manage and mitigate risks associated with offshoring and cloud computing.

6.2.4 Risks must be adequately understood and managed prior to entering into an offshoring and cloud computing arrangement. Factors that must be addressed include, inter alia, continuity, data protection, regulatory access to data and regulatory compliance.

6.3 Business continuity plan

6.3.1 A reporting entity must satisfy itself that the data centre hosting the data must have extensive disaster recovery and business continuity processes and procedures in place.

6.3.2 Regular disaster recovery tests must be performed to ensure data can be recovered.

6.4 Storage of data

6.4.1 All FinSurv related data must be ring-fenced without the ability to be updated by unauthorised persons.

6.4.2 Cross-border transactional data must be stored directly into the source system, i.e. the core accounting system.

6.4.3 Customer data must be stored directly from the source system, i.e. the centralised customer database.

6.4.4 In an event of the reporting entity terminating its operations in South Africa for any reason whatsoever, data for five years preceding the date of termination, must be replicated to South Africa by the reporting entity in a format accessible by FinSurv and within an agreed period.

6.5 Regulatory access to data

6.5.1 Any data required by FinSurv must be made available for access immediately, but not later than 48 hours, by the reporting entity and should forthwith be furnished to FinSurv in the format prescribed in paragraph 6.8.7 below.

6.5.2 Information must be made available, upon request, at no cost to FinSurv.

6.5.3 The use of offshoring and cloud computing may not in any way infringe on FinSurv's mandated access to data.

6.6 Jurisdiction

6.6.1 A reporting entity must ensure that data is not stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

6.6.2 In considering foreign jurisdictions, a reporting entity must take into account the wider political and security stability of the particular jurisdiction as well as the legislative requirements in terms of the foreign jurisdiction concerned. This should include consideration of the legal enforcement provisions within a jurisdiction.

6.7 Procedure to update data back to source

6.7.1 From time to time a reporting entity may be required to amend certain data, e.g. balance of payments categories or cancel the reporting of a transaction. This might have an impact on FinSurv's same source reporting principle, as all changes must be updated back to the source, i.e. transactional or accounting system.

6.8 System requirements

6.8.1 Data in any offshore data centre must at the least be encrypted through modern encryption technology.

6.8.2 All cryptographic keys used in a storage encryption solution must be secured and managed properly to support the security of the solution.

6.8.3 To prevent the non-recovery of encrypted data, extensive planning of key management processes, procedures, and technologies should be performed before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery and destruction.

6.8.4 Only authorised personnel and systems must be able to retrieve, decrypt and process data through any network or cloud.

6.8.5 The foreign service provider should have very strong, documented and tested cyber controls to protect data against cybercrime.

6.8.6 A reporting entity must verify adherence to the agreed information security requirements, i.e. through third party assurance audits and/or any other security testing requirements such as vulnerability scanning and penetration testing.

6.8.7 Data requested by FinSurv should be provided in a standard report format, as prescribed in the Authorised Dealer Manual and ADLA Manual, such as a semi-colon delimited file (e.g.CSV).

6.9 Other regulatory bodies and legislative requirements

6.9.1 This position paper is not exhaustive, nor should it be read in isolation and a reporting entity must consider this position paper in the context of its overarching regulatory obligations, which may include obligations to the Financial Intelligence Centre and the Prudential Authority who have different statutory objectives and may, therefore, have different requirements.

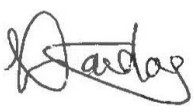
6.9.2 A reporting entity must acquaint itself with the relevant provisions of the applicable legislation, e.g. the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (POPIA) and Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001).

7. Assurances

7.1 The compliance with all the requirements listed in paragraph 6. above, must be contained in the Managerial Letter of Comfort to be provided to FinSurv on an annual basis, as prescribed in the Authorised Dealer Manual and ADLA Manual.

8. Remedies

8.1 Any failure by a reporting entity to comply with FinSurv's above-mentioned requirements may result in the suspension of authorities provided by FinSurv or may cause FinSurv to invoke remedies available to it in terms of the Exchange Control Regulations.



K Naidoo
Deputy Governor and CEO: Prudential Authority

Date: 25 August 2020