

CLOUD COMPUTING AND DATA OFFSHORING IN THE NATIONAL PAYMENT SYSTEM

National Payment System Department

Consultation paper – March 2025



SOUTH AFRICAN RESERVE BANK



CONTENTS

1.	Definitions	3
2.	Background and introduction	5
3.	Problem statement	6
4.	Purpose	7
5.	Overview of cloud computing and data offshoring	7
6.	Benefits of cloud computing and data offshoring	13
7.	Risks associated with cloud computing and data offshoring	16
8.	Overview of interventions on cloud computing and data offshoring in selected jurisdictions and standard-setting bodies	23
9.	Policy and regulatory recommendations for the use and adoption of cloud computing and data offshoring in the NPS	33
10.	Questionnaire	47
11.	Conclusion	49
12.	Comments, consultation questions and contact details	50
	ABBREVIATIONS	51

1. Definitions

- 1.1 This section of the consultation paper defines the terms used in this paper. If a term is not defined in this section, then the definitions are aligned with the South African Reserve Bank (SARB) National Payment System Department's (NPSD) policy papers, position papers, information papers, interpretation notes and directives as well as the National Payment System Act 78 of 1998, as amended (NPS Act).
- 1.2 **Cloud computing:** means a model for enabling convenient, on-demand network access to a shared pool of configured computer resources (e.g. network, servers, storage facilities, application and other services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.¹
- 1.3 **Community cloud:** means a cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organisations with shared concerns (e.g. in terms of mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more organisations in the community, a third party or some combination of them, and it may exist on or off premises.
- 1.4 **Critical payment data, processes, activities and service:** means data, processes, activities and service whose failure or disruption could significantly impair an operator and payment institution's viability, critical operations and functions and/or ability to meet its key legal, regulatory and supervisory obligations.
- 1.5 **Critical service provider:** means a service provider that provides critical services to a payment institution and operator in the national payment system (NPS).

¹ See Bank For International Settlements (BIS) Regulating and supervising the clouds: emerging prudential approaches for insurance companies : [FSI Insights on policy implementation](#)

- 1.6 **Data offshoring:** means the storing and processing of data outside of the Republic of South Africa.
- 1.7 **Hybrid cloud:** means cloud infrastructure composed of two or more distinct cloud infrastructures (e.g. a public and a private cloud).
- 1.8 **National payment system (NPS):** means the system in the Republic of South Africa that enables the flow of funds from a payer to a payee and encompasses the total payment process in the Republic, including the payment, clearing and settlement systems, infrastructures, mechanisms, institutions, activities, agreements, procedures, rules and laws.
- 1.9 **Nearshoring:** means the storage and processing of data in nearby and bordering regions and countries, e.g. the Common Monetary Area (CMA) countries and the Southern African Development Community (SADC) countries.
- 1.10 **Onshoring:** means the storage and processing of data at a lower-cost location in the Republic of South Africa, a third-party service provider or a parent organisation in South Africa.
- 1.11 **Payment institution:** means persons designated, authorised, registered or regulated under the National Payment System Act 78 of 1998 (NPS Act), including but not limited to clearing system participants, settlement system participants, third-party payment providers and system operators.
- 1.12 **Payment system Financial Market Infrastructure:** means a multilateral system among payment system participants, including the operator of the system, used for the purposes of clearing, settling or recording payments, and includes a systemically important payment, clearing or settlement system and a prominent payment, clearing or settlement system.

- 1.13 **Operator:** means an operator of a payment system, including payment clearing house system operators, operators of settlement systems and the operator(s) of payment system financial market infrastructures (FMIs).
- 1.14 **Private cloud:** means cloud infrastructure available for the exclusive use by a single institution or payment institution and operators.
- 1.15 **Public cloud:** means cloud infrastructure available for open use by the general public.
- 1.16 **Service provider:** means any party which provides a service to the payment institution and operators, whether the party is within or outside the borders of South Africa.
- 1.17 **Vendor lock-in:** means to a situation where a payment institution and operator is unable to easily change its cloud service provider due to the terms of a contract, a lack of feasible alternative providers, technical features or vendor portability.

2. Background and introduction

- 2.1 The adoption of cloud-computing and data-offshoring services by payment institutions and operators in the NPS has rapidly increased with technological advances and the ever-changing payment landscape. Cloud computing offers several advantages, such as economies of scale, flexibility, operational efficiencies and resilience, and cost-effectiveness for payment institutions and operators. Data offshoring enables payment institutions and operators to efficiently transmit and store data offshore (globally/outside of the borders of South Africa), and provides payment-related services, activities and products domestically and internationally. However, cloud computing and data offshoring also pose challenges in terms of data protection and location as well as operational, reputational,

concentration, systemic and cybersecurity risks for payment institutions, operators and the broader NPS.

- 2.2 Various domestic and global financial sector regulators have different approaches to cloud computing and data offshoring. As the NPS regulator, the SARB's NPSD² does not have a cloud-computing policy position or regulatory framework, which leads to policy and regulatory uncertainty relating to cloud computing and data offshoring in the NPS. To address this uncertainty, the SARB is developing a policy position and regulatory framework for cloud computing and data offshoring in the NPS. This consultation paper seeks to propose the NPS cloud-computing and data-offshoring policy and regulatory framework, and to solicit inputs from the industry on the proposed policy and regulatory framework for cloud computing and data offshoring in the NPS.

3. Problem statement

- 3.1 There is no explicit policy or regulatory framework in the NPS relating to cloud computing and data offshoring for payment institutions and operators. In 2018, the SARB issued a position paper formally supporting the Principles for Financial Market Infrastructures (PFMI) issued by the Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures (CPMI) together with the International Organization of Securities Commissions (IOSCO), referred to as the *Position paper on the Principles for Financial Market Infrastructures*³. The PFMI do not specifically provide principles or standards for cloud computing and data offshoring. However, the PFMI provide guiding principles on operational resilience, outsourcing and third-party relationships for FMIs that may also apply to cloud computing and data offshoring.

² In terms of section 10(1)(c) of the South African Reserve Bank Act 90 of 1989, as amended (SARB Act), the South African Reserve Bank (SARB) is required to perform such functions, implement such rules and procedures, and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems.

³ See Position Paper on the Principles for Financial Market Infrastructures: [Position Paper on the Principles for Financial Market Infrastructures](#)

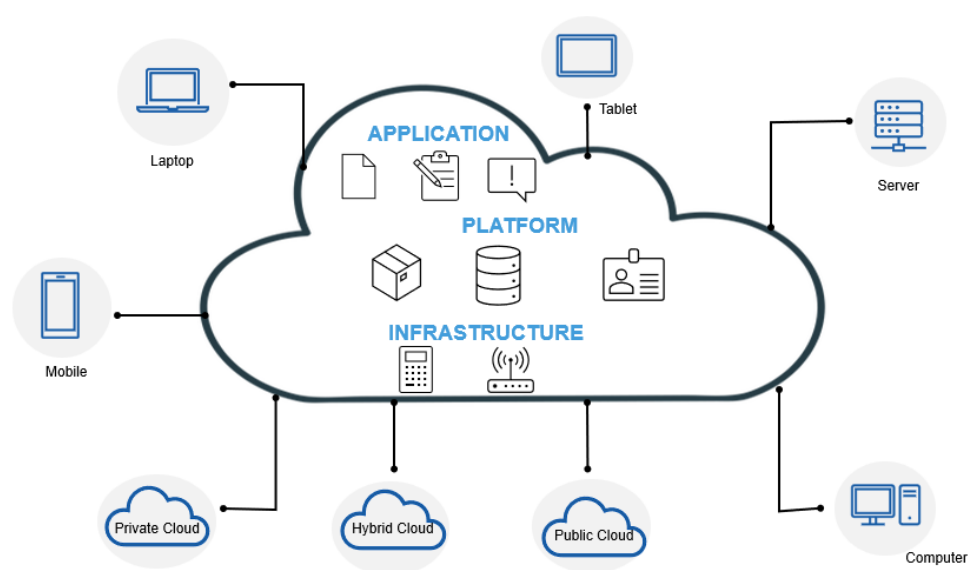
4. Purpose

- 4.1 The purpose of this consultation paper is to propose a policy and regulatory framework for cloud computing and data offshoring for payment institutions and operators in the NPS and to solicit inputs from the industry and other stakeholders.

5. Overview of cloud computing and data offshoring

- 5.1 This section of the consultation paper provides an overview and background of cloud computing and data offshoring based on research. Figure 1 defines cloud computing and the various use cases for cloud computing. Figure 2 defines data offshoring and the several ways to outsource data. Table 1 provides an overview of the type of cloud deployment model or cloud computing architecture that the cloud service provider could deploy for a payment institution and operators, for example on a public cloud, a private cloud, a community cloud or a hybrid cloud. Lastly, Table 2 and Figure 3 discusses cloud-computing services, namely infrastructure as a service, platform as a service, software as a service and business process as a service.

Figure 1: Cloud computing



5.2 In simple terms, cloud computing is the delivery of computing services – including servers, storage, databases, networking, software, analytics and intelligence over the Internet ('the cloud') – on a pay-as-you-go basis to offer faster innovation, flexible resources and economies of scale. Instead of buying, owning and maintaining physical data centres and servers, payment institutions and operators can access technology services – such as computing power, storage and databases – on an as-needed basis from a cloud service provider.

5.3 **Uses of cloud computing**

5.3.1 **Design and develop cloud-native applications:** Payment institutions and operators can efficiently construct, deploy and expand applications across web, mobile and Application Programming Interface (API) application platforms by harnessing the power of cloud-native technology and methodology.

5.3.2 **Store, back up and recover data:** Payment institutions and operators can safeguard data more economically and extensively by securely transmitting it over the Internet to a remote cloud storage system. The payment institution and operators can access the cloud system anywhere – on any device, infrastructure and system.

5.3.3 **Gain broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops and workstations).

5.3.4 **Stream audio and video:** Payment institutions, operators and customers can experience seamless audio and video content streaming. The payment institution and operators can connect effortlessly with its customers and audience, regardless of their location or device. Customers can easily enjoy crystal-clear audio as well as high-quality, high-definition videos, reaching a global audience.

- 5.3.5 **Deliver software on demand:** Also known as software as a service (SaaS), on-demand software enables payment institutions and operators to deliver the newest software versions and updates to customers whenever and wherever required.
- 5.3.6 **Build and test applications:** Payment institutions and operators can reduce cost and time in application development by leveraging cloud infrastructures that offer easy scalability.
- 5.3.7 **Pool resources:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the payment institutions and operator's demand.
- 5.3.8 **Analyse data:** Payment institutions and operators can leverage cloud technology to consolidate and integrate data from various teams, divisions and locations. Then they can harness the power of cloud services like machine learning and artificial intelligence (AI) to extract valuable insight and make well-informed decisions based on data analysis.
- 5.3.9 **Embed intelligence:** Payment institutions and operators can use sophisticated models to engage clients and extract meaningful insight from captured data.
- 5.3.10 **To conclude:** various organisations, companies, regulators, governments and the public use an online service to send emails, edit documents, watch movies or television, listen to music, play games or store pictures and other files using cloud computing.

5.4 **Data offshoring:** This refers to the storing and processing of data outside of the Republic of South Africa. Some payment institutions and operators are offshoring their data through an insourcing relationship with their parent organisation or offshoring the data to a third-party or cloud service provider.



Figure 2: Data offshoring

5.5 **Types of outsourcing for data storage and processing:** There are several ways to outsource data depending on the business operations of payment institutions and operators. Broadly speaking, there are a few differences in types of outsourcing based on the distance between the payment institutions, operators and the third-party service provider or parent organisation. These types are:

5.5.1 **Onshoring:** storages and processing of data at a lower-cost location in South Africa, a third-party service provider or a parent organisation in South Africa.

5.5.2 **Offshoring:** storages and processing of data outside of South Africa to third-party service providers or a parent organisation.

5.5.3 **Nearshoring:** storages and processing of data in nearby and bordering regions and countries, e.g. CMA and SADC countries.

5.6 Payment institutions and operators need to determine the type of cloud deployment model, or cloud computing architecture, on which the service provider will implement the cloud services. There are four different ways to deploy cloud services: on a public cloud, a private cloud, a community cloud or a hybrid cloud, – as discussed below:

Table 1: Cloud deployment modules

Public cloud ⁴	Private cloud ⁵	Community cloud ⁶	Hybrid cloud ⁷
<p>a) Public clouds are the most common type of cloud-computing deployment. The cloud resources (e.g. servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. With the public cloud, the cloud provider owns and manages all hardware, software and other supporting infrastructure.</p> <p>b) With the public cloud, payment institutions and operators share the same hardware, storage and network devices with other institutions or cloud ‘tenants’. Payment institutions and operators can access services and manage their accounts using a web browser.</p>	<p>a) A private cloud consists of cloud-computing resources used exclusively by one payment institution and operator. A private cloud may be owned, managed and operated by the payment institution, operator, a third-party cloud service provider or a combination of both.</p> <p>b) A private cloud can be located on-premises of a payment institution, operators or off-premises hosted by a third-party cloud service provider.</p> <p>c) The services and infrastructure are always maintained on a private network with the private cloud, hardware and software dedicated solely to the payment institution and operator.</p>	<p>a) A community cloud is when a cloud service provider provisions the cloud infrastructure for exclusive use by a specific community such as payment institutions and operators in the NPS. The community usually has a common goal, for example the safety and efficiency of the NPS, innovation, shared data, shared services, and shared regulatory and supervisory requirements.</p> <p>b) A community cloud may be owned, managed and operated by one or more payment institutions and operators in the NPS, “the community” itself, a cloud service provider or a combination thereof. A community cloud can exist on or off the premises of the payment institutions and operators.</p>	<p>a) A hybrid cloud combines on-premises infrastructure or a private cloud with a public cloud or a community cloud, which becomes a composition of two or more distinct cloud infrastructures (public, private or community) that remain unique to the payment institutions and operators but are bound together by standardised or proprietary technology that enables data and application portability.</p> <p>b) Hybrid clouds allow data and applications to move between the two environments. Many financial institutions choose a hybrid-cloud approach due to the financial landscape, such as meeting regulatory requirements and data laws.</p>

⁴ See: [What is a Private Cloud - Definition | Microsoft Azure](#)

⁵ See: <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/What is a Public Cloud - Definition | Microsoft Azure>

⁶ See: <https://www.spiceworks.com/tech/cloud/articles/what-is-community-cloud/>

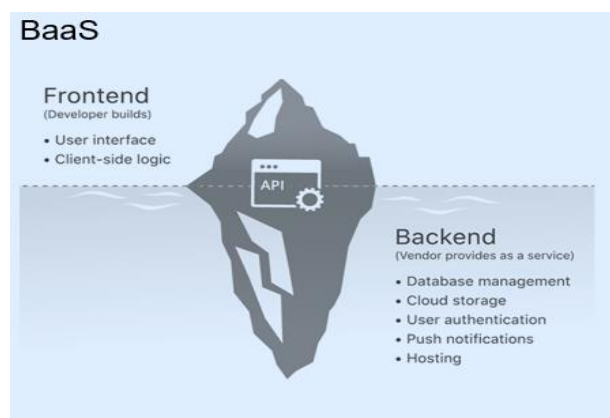
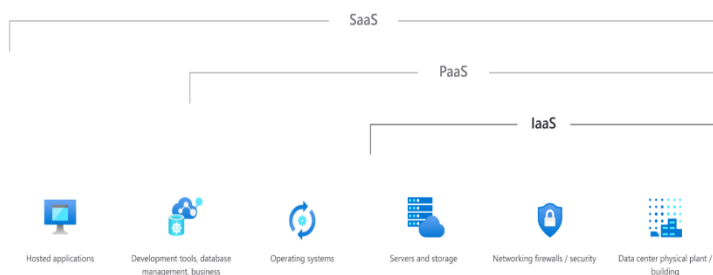
⁷ See: [What is Hybrid Cloud Computing – Definition | Microsoft Azure](#)

5.7 Most cloud-computing services fall into four broad categories, namely infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) and business process as a service (BPaaS), which are discussed below.

Table 2: Type of cloud-computing services⁸

Infrastructure as a service (IaaS)	Platform as a service (PaaS)	Software as a service (SaaS)	Business process as a service (BPaaS)
IaaS is a model of cloud service where customers are supplied with information technology (IT) infrastructure, provided and managed over the internet on a pay-as-you-use basis (e.g. servers and storage).	PaaS is a model of cloud service where customers are supplied with an on-demand environment for developing, testing, delivering and managing software applications over the Internet.	SaaS is a model of cloud service allowing customers to connect to and use cloud-based applications over the Internet on a subscription basis.	BPaaS ⁹ is an automated business process delivered from a cloud service. BPaaS usually has a well-defined interface which makes it easy to be used by different enterprises.

Figure 3: Type of cloud-computing services¹⁰



Source: Financial Stability Board Third-party dependencies in cloud services and Cloudflare

⁸See: <https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/>

⁹ See: [What is BaaS? | Backend-as-a-Service vs. serverless | Cloudflare](#)

¹⁰ See Financial Stability Board Third-party dependencies in cloud services: [Third-party dependencies in cloud services](#)



6. Benefits of cloud computing and data offshoring

6.1 **Lower costs, scalability and efficiency¹¹:** Cloud computing and data offshoring may contribute to lower technological infrastructure costs by transforming large upfront capital expenditures into smaller ongoing operational costs. Deploying a server and data on a cloud is faster than deploying a server and data in a traditional data centre. Upgrading conventional IT infrastructures and data centres is time-consuming, costly and resource-intensive. Moreover, integrating new payment technologies into traditional infrastructures and data centres is a long and expensive process. Offshoring can potentially lead to significant business cost savings as payment institutions and operators can take advantage of lower labour and other production costs in another country. Offshoring can also lead to increased efficiency as payment institutions and operators can take advantage of the latest technology and processes available in another country.

6.2 **Competition and innovation:** The adoption of cloud-computing and data-offshoring services in the NPS may create a level playing field between large payment institutions, operators and small to medium payment institutions and operators. Access to extensive computing infrastructure,

¹¹ Cloud computing may offset initial capital expenditure; however, the variable usage-based costing may lead future expected costs.

data centres and resources was previously only available to larger payment institutions with the ability to devote significant capital and resources to technology infrastructure and data centres. In addition, the lower upfront cost of cloud computing and data offshoring makes it easier for new small to medium payment institutions, operators and financial technology (fintech) start-ups to compete with the incumbent payment institutions and operators. This results in increased competition in the NPS, increases the quality and number of innovative payment services and products offered to consumers, and increases financial inclusion and broader consumer reach.

6.3 Enhanced cross-border payments: Deploying payment services and systems data on a cloud and offshore, and using cloud service providers or their offshore parent organisation, enables payment institutions and operators to expand globally and easily deploy and have access to applications in multiple regions around the world, which may enhance cross-border payments. Enhancing cross-border payments' speed and transparency while increasing access to cross-border payment services and reducing costs are the key objectives of the Group of Twenty (G20) cross-border payments programme.¹²

6.4 Increased security and resilience: Cloud service providers can contribute to the security and cyber-resilience of payment institutions and operators where cloud service providers¹³ prioritise cloud security implementation and research. According to the Financial Stability Board's (FSB) consultation feedback on the regulatory and supervisory issues relating to outsourcing and third-party relationships,¹⁴ some respondents noted that the quality of the services delivered by a service provider (e.g. a cloud service provider) is dependent on its ability to appropriately protect the confidentiality, integrity and availability of the data as well as the security and reliability of the systems used to process, transfer or store data. Ensuring cybersecurity and an appropriate level of data protection is a challenge for financial

¹² See BIS Enhancing cross-border payments: building blocks of a global roadmap: [Enhancing cross-border payments](#)

¹³ Smaller cloud service providers may not prioritise cloud security implementation and research.

¹⁴ See Public responses to the Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: [Discussion paper](#)

institutions and some third-party service providers. Institutions that place reliance on services provided by third parties (e.g. for cloud services) can enhance the cybersecurity of financial institutions relative to their on-premises information and communication technology (ICT) infrastructure where cloud service providers are at the forefront of security implementation and research.

- 6.5 **Time-zone differences and locations¹⁵:** Data storage and processing through a cloud service provider or data offshoring to an offshore parent organisation can assist with increased availability (e.g. 24/7 capacity¹⁶) and business continuity planning (BCP) as the offshore teams can cover time zones not covered by the onshore teams or in the event of operational failures or events impacting on the onshore teams (e.g. an electricity blackout or severe climate-change event in South Africa such as wildfires, floods or earthquakes). Multiple teams working in different countries can help reduce operational risk.
- 6.6 **Access to global skills and talent:** Cloud computing and data offshoring can enable payment institutions and operators to access global payment skills, talent and resources from the cloud service provider, third-party provider or parent organisation to improve the quality of services offered.
- 6.7 **Increased agility and flexibility:** Cloud computing and data offshoring can lead to increased agility and flexibility for payment institutions and operators to respond quickly to changes in demand and market conditions.
- 6.8 Overall, data offshoring can be a beneficial strategy for payment institutions and operators, providing them with cost savings, access to new markets and talent, increased efficiency and greater flexibility.

¹⁵ A cloud-agnostic setup is an added benefit, where the aim is to avoid vendor lock-in and leverage multiple cloud providers. Managing data storage and processing across different time zones and locations can enhance availability and resilience with geo-redundancy.

¹⁶ 24 hours a day, 7 days a week.

7. Risks associated with cloud computing and data offshoring

- 7.1 **Operational risk:** The use of cloud computing, reliance on cloud-computing service providers and data offshoring may result in payment institutions and operators facing additional operational risk emanating from the service provider or their offshore parent organisation. The operational risks could emanate from deficiencies in information systems or internal processes, human errors, management failures or disruptions from external events that can result in the reduction, deterioration or breakdown of services which payment institutions and operators require from the service provider or parent organisation. This will impact on the payment institutions and operator's operational capacity to provide licensed, registered, designated or authorised activities. In the event that the service provider serves more than one payment institution and operator in the NPS, the operational risk may affect the safety and efficiency of the NPS and could result in systemic risk.
- 7.2 **Reputational risk:** South Africa has a world-class NPS, and its payment institutions and operators have maintained and supported the safety and efficiency objectives of the NPS alongside other SARB objectives. Adopting cloud computing, cloud-computing service providers in the NPS and data offshoring without a policy and regulatory framework that supports the safety and efficiency objectives could result in reputational risk for the SARB and payment institutions and operators.
- 7.3 **Complexity and lack of transparency:** The FSB has noted that outsourcing, data offshoring and third-party relationships, which include cloud service providers, are complex and lack transparency.¹⁷ Therefore, it is difficult or even impossible for operators, payment and financial institutions to influence service providers' subcontracting' decisions, making it very challenging for operators, payment and financial institutions

¹⁷See FSB Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships: [Regulatory and Supervisory Issues](#)

to manage and mitigate supply-chain risks. In addition, operators, payment and financial institutions as well as authorities are currently unable to ‘map’ the entities and activities involved in third parties’ supply chains and to appropriately assess the impact of supply-chain disruption on operators, payment and financial institution’s resilience.

7.4 Concentration risk: A few multinational companies operate in the cloud-computing market, which may expose the NPS to concentration risk¹⁸. If payment institutions and operators increase their reliance on cloud computing and cloud-computing service providers for core payment services, activities and operations, outages from the service provider could lead to system-wide disruptions in the NPS. Furthermore, payment institutions, operators and the SARB do not have data on the interdependencies of concentrated cloud service providers or other offshore service providers and their preparedness for outages and therefore cannot monitor the risks. In addition, payment institutions and operators may be unable to substitute certain technologies or services provided by cloud service providers or other service providers in a cost-efficient and timely manner and without risks and disruption, mainly if the service provider or cloud service provider is located in other jurisdictions.

7.5 Vendor lock-in risk: This is where a payment institution and operator cannot easily change its service provider due to the terms of a contract, a lack of feasible alternatives or technical features. For example, vendor lock-in risk could occur if a payment institution and operator’s agreement with a cloud service provider or an offshore service provider prevents the orderly transfer of payment services and activities to another service provider or other payment institutions and operators in the event of the termination of the agreement and/or a severe disruption of service.

7.6 Systemic risks: Concentration in the provision of cloud-computing services, the use of cloud service providers or the use of offshore service

¹⁸ The concentration risk potentially introduces targeted cyberattacks. Cloud providers supporting a NPS could become targets for cyberattacks, and a successful breach could compromise sensitive data, undermining trust in the NPS.

providers in the financial sector globally, especially the outsourcing of critical services to service providers, poses systemic risks. This systemic risk is increasing as more operators, payment and financial institutions migrate their critical services to a cloud or offshore data using service providers for core services and activities previously performed by the operators, financial and payment institutions themselves.

- a) Systemic risk could occur if many payment institutions, operators or systemically important payment institutions depend on only one or a few service providers to provide critical payment services and operations or offshore critical payment services, data and/or processes. In the event of a significant disruption, outage or failure at a service provider or their offshore parent organisation, this could create a single point of failure with potentially adverse consequences for the financial stability, safety and efficacy of the NPS as well as the safety and soundness of multiple payment institutions and operators.

7.7 The lack of Internet connection: Cloud computing and data offshoring relies 100% on the Internet, and a strong Internet connection is the most important requirement for the cloud and offshoring processes to function sufficiently. This might be an obstacle for payment institutions and operators located in areas where their systems lack connection stability or are impacted by the electricity cuts in South Africa, and result in poor network and Internet connectivity.

7.8 Cloud and offshoring security threats: The adoption of cloud computing and data offshoring by payment institutions and operators results in a high volume of sensitive data flowing between the payment institutions, operators and the service providers or their offshore parent organisation, which generates opportunities for accidental and malicious leaks of sensitive data to untrusted third parties. Human errors, insider threats, malware, weak credentials and hackers contribute to most data breaches, and sophisticated hackers use their expertise to target cloud systems or data systems and gain access. Hackers employ social engineering,

account takeovers, lateral movements and detection evasion tactics to maintain a long-term presence on the victim organisation's network, often using the built-in tools from cloud services. Their goal is to transfer sensitive information to systems under their control.¹⁹

- a) The quality of the services delivered by cloud service providers, other offshore service providers or their offshore parent organisation depends on the ability to appropriately protect the confidentiality, integrity and availability of the data as well as the security and reliability of the systems used to process, transfer or store the data.

7.9 **Maintaining relevant ICT resources and skills:** With the migration and adoption of cloud computing and data offshoring, payment institutions and operators now rely on ICT resources and skills provided by cloud service providers, other offshore service providers or their offshore parent organisation. In future, payment institutions and operators may experience a shortage of appropriate ICT resources and skills to effectively address the evolving payment landscape. The FSB has highlighted that recruiting, retaining and training employees with the relevant experience and skills to effectively manage the risk from the growing range of third-party ICT service providers is a challenge for operators, payment and financial institutions as well as for the supervisory and resolution authorities overseeing them.²⁰

7.10 **Dependence on other countries' geographical, political and legal risks:** Cloud computing and data offshoring in the NPS could make South African payment institutions and operators overly dependent on other countries for operating payment systems and processing payment data in South Africa.

7.10.1 Cloud service providers and data-offshoring service providers that diversify their data centres in terms of geographical location must ensure sufficient redundancy within each centre to ensure that the impact of an incident

¹⁹ See Vectra Cloud security: [Cloud security](#)

²⁰ See FSB Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships: Regulatory and Supervisory Issues: [Regulatory and Supervisory Issues](#)

would not cause system-wide spillovers. Also, legal challenges may arise in the cross-border provision of cloud services and data offshoring. For example, there may be uncertainties over the legal obligations under foreign law of service providers operating on a cross-border basis, either regarding access to and use of data or regarding their continuing to provide services to payment institutions and operators in South Africa in case of geopolitical issues or sanctions. With respect to legal risk, there are also issues with liability as some providers in South Africa lease their data centres and do not own them, making it difficult to determine where liability lies.

- a) The highest risk in cloud computing involves geopolitical tensions. This includes potential compromises in the host country of the data or directives to cloud service providers based on their domicile legislation. Given the dominance of United States (US) and Chinese cloud service providers, South African entities should mitigate risks by either maintaining minimum essential loads/copies within South Africa or diversifying cloud service provider portfolio to include both Eastern and Western companies.
- b) With South Africa being a player, especially recently, in legal proceedings with some countries, it would be prudent for payment institutions and operators to be aware that partner states hold a significant portion of control over cloud-computing infrastructure around the world.
- c) The Department of Communications and Digital Technologies (DCDT) has noted that South Africa and other African countries have unequal participation in data centres (see Figure 4), with the possible implication that data generated in African countries (including in South Africa) is mostly stored in other jurisdictions and, where it is stored locally, it is owned by giant IT companies.²¹

²¹ See DCDT Draft National Policy on Data and cloud: [Draft National Policy](#)

Figure 4: Geographical distribution of co-location data centres, February 2019 – By Country

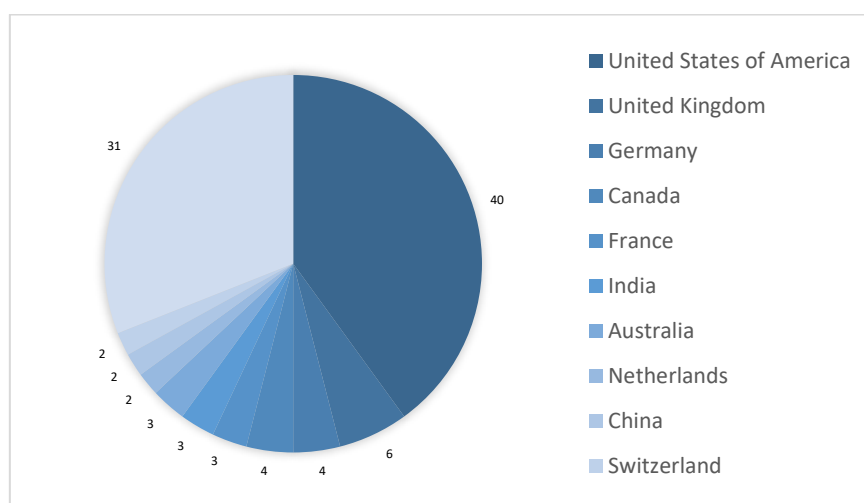
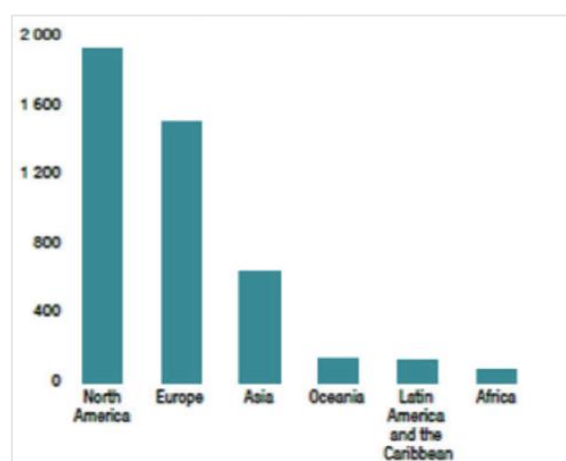


Figure 5: Geographical distribution of co-location data centres, February 2019 – By Region



Source: United Nations Conference on Trade and Development (UNCTAD) 2019 Report

- d) Furthermore, the DCDT acknowledges that data storage is not limited to geographical location, necessitating due consideration measures which ensure that cross-border data transfers do not transgress the national security and privacy protection laws and other related policies and legislation of South Africa.

7.11 **Supervisory and regulatory challenges:** The SARB requires access to data and records to effectively regulate, oversee and supervise payment

systems, payment institutions and operators. Offshoring data to locations outside of the borders of South Africa may hamper the SARB's ability to exercise its mandate on payment systems, payment institutions and operators. The SARB may find it challenging to access offshored data as the location of the data or where the data is processed may fall outside of the jurisdiction and regulatory scope of the SARB. In addition, many national regulators are concerned that, once data has left the borders of their jurisdiction, they may not have the power to access it again.²²

7.12 Data protection risk: Data could be stored or processed in other jurisdictions where South African laws on data protection do not apply. These laws include the provisions of the Protection of Personal Information Act 4 of 2013 (POPI Act), the NPS Act, all the regulatory instruments issued in terms of the NPS Act, other financial sector laws and PCH SO criteria.²³ Therefore, the data regulations in different jurisdictions may be inconsistent with or provide less protection than the POPI Act and other local data protection regulations in the NPS and financial services industry.

²² The other concern is that foreign entities could subpoena South African data to pursue their agendas, for example: in response to 9/11, the US government created [The Patriot Act](#), providing their agencies with access to not only personal data but also all organisation's data that met the requirements set out by the Act.

²³ At present, there are four authorised PCH SOs, namely (i) BankservAfrica; (ii) Visa Limited (Visa); (iii) MasterCard Limited (MasterCard) all for retail payments; and (iv) Strate for equities, bonds and money market instruments. The Payments Association of South Africa (PASA) authorises PCH SOs to provide clearing services. Currently, the agreements, rules and procedures as well as the criteria for PCH SOs are formulated and managed by PASA, with the approval of the SARB.


8. Overview of interventions on cloud computing and data offshoring in selected jurisdictions and standard-setting bodies

8.1 This section of the consultation paper provides an overview of a few jurisdictions and standard-setting bodies' regulatory interventions on cloud computing and data offshoring.

Jurisdiction		Regulatory intervention
CPMI-IOSCO		<p>The CPMI-IOSCO's PFMI do not specifically provide standards for cloud services. However, since the PFMI are principles-based, the guidelines on outsourcing and third-party relationships also apply to FMIs' cloud outsourcing where relevant. The CPMI-IOSCO's <i>Guidance on cyber resilience for financial market infrastructures</i>²⁴ provides supplemental guidance to the PFMI on cyber-risk. It addresses risk in relation to data, interconnections with service providers and outsourcing.</p>
European Union (EU)		<p>In 2019, the European Banking Authority (EBA) updated its Committee of European Banking Supervisors (CEBS) guidelines on outsourcing²⁵ that had been issued in 2006, which applied exclusively to credit institutions. The aim is to establish a more harmonised framework for all financial institutions that are within the scope of the EBA's mandate, namely credit institutions and investment firms as well as payment and electronic-money institutions. The guidelines set out specific provisions for these financial institutions' governance frameworks with regard to their outsourcing arrangements and the related supervisory expectations and processes. The recommendation on outsourcing to cloud service providers, published in December 2017, has been integrated into the guidelines.</p> <p>Data offshoring: With regard to outsourcing to service providers located in third countries, financial institutions are expected to take particular care that compliance with European Union (EU) legislation and regulatory requirements (e.g. professional secrecy, access to information and data, and the protection of personal data) is ensured and that the competent authority is able to effectively supervise financial institutions, in particular regarding critical or important functions outsourced to service providers.</p> <p>IT outsourcing, including fintech and the outsourcing to cloud service providers: Institutions and payment institutions must ensure that personal data is adequately protected and kept confidential. Institutions and payment institutions fall within the scope of application</p>

²⁴See Third-party dependencies in cloud services: Considerations on financial stability implications: [Third-party dependencies in cloud services](#)

²⁵See Guidelines on outsourcing arrangements: [Guidelines on outsourcing arrangements](#)

		<p>of Regulation (EU) 2016/67917 (General Data Protection Regulation (GDPR)²⁶) and must comply with it. When outsourcing IT or data services, it is imperative that business continuity and data protection are appropriately considered. Such considerations are not limited to the outsourcing of IT but apply in general. Institutions and payment institutions must ensure that they meet internationally accepted information security standards, and this also applies to outsourced IT infrastructures and services.</p> <p>The Digital Operational Resilience Act (DORA)²⁷ is an EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025. It aims to strengthen the IT security of financial entities such as banks, insurance companies and investment firms, and to ensure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption. DORA harmonises the rules relating to operational resilience for the financial sector, applying to 20 different types of financial entities. DORA covers the following:</p> <ul style="list-style-type: none"> • ICT risk management: the principles and requirements on an ICT risk management framework; • ICT third-party risk management: monitoring third-party risk providers and key contractual provisions; • digital operational resilience testing: basic and advanced testing; • ICT-related incidents: general requirements for the reporting of major ICT-related incidents to competent authorities; • information sharing: the exchange of information and intelligence on cyber-threats; and • Oversight of critical third-party providers: an oversight framework for critical ICT third-party providers. <p>The three European supervisory authorities a – namely the EBA, the European Insurance and Occupational Pensions Authority (EIOPA) as well as the European Securities and Markets Authority (ESMA – are preparing a set of policy products to enable the application of DORA.</p>
Financial Stability Board (FSB)		<p>In 2020, the FSB published a discussion paper considering the regulatory and supervisory issues relating to outsourcing and third-party relationships²⁸ which included cloud computing and computing service providers. The FSB's Standing Committee on Supervisory and Regulatory Cooperation (SRC) conducted a survey of the existing regulatory and supervisory landscape relating to outsourcing and third-party risk management in its member jurisdictions' financial institutions. The survey covered various aspects of the regulation and supervision of</p>

²⁶ See Legal framework of EU data protection: [Legal framework of EU data protection](#)

²⁷ See Digital Operational Resilience Act (DORA): [Digital Operational Resilience Act](#)

²⁸ See FSB Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships: Regulatory and Supervisory Issues: [Regulatory and Supervisory Issues](#)

		<p>financial institutions' outsourcing and third-party relationships, including governance and risk management; cyber, data and information security; access, audit and information rights; and BCP and exit strategies. The discussion paper:</p> <ol style="list-style-type: none"> 1. provided a high-level overview of the existing regulatory and supervisory landscape based on the survey findings as well as some preliminary observations from authorities and financial institutions' responses to the COVID-19 pandemic; 2. briefly described various regulatory and supervisory approaches for managing outsourcing and third-party risks in SRC member jurisdictions; 3. listed some common regulatory and supervisory challenges; and 4. identified issues for further exploration. <p>The discussion paper encouraged dialogue among financial institutions, supervisory authorities and third parties on the challenges in identifying and managing the risks relating to their outsourcing and third-party dependencies. It also set out some additional issues relating to outsourcing and third-party risk management in the financial sector which the COVID-19 pandemic had highlighted, and invited views from financial institutions and third parties. In 2021, the FSB published the outsourcing and third-party risk: overview of responses for public consultation.²⁹</p> <p>In June 2023, the FSB published, for public consultation, a toolkit for financial authorities and financial institutions as well as service providers for their third-party risk management and oversight.³⁰ The toolkit aims to:</p> <ol style="list-style-type: none"> 1. reduce fragmentation in regulatory and supervisory approaches to financial institutions' third-party risk management across jurisdictions and different areas of the financial services sector; 2. strengthen financial institutions' ability to manage third-party risks and financial authorities' ability to monitor and strengthen the resilience of the financial system; and 3. facilitate coordination among relevant stakeholders (i.e. financial authorities, financial institutions and third-party service providers).
--	--	--

²⁹ See Outsourcing and third-party risk – Overview of responses to the public consultation: [Overview of responses to the public consultation](#)


³⁰ See FSB Enhancing Third-Party Risk Management and Oversight: [Enhancing Third-Party Risk Management and Oversight](#)

Hong Kong		In August 2020, the Hong Kong Monetary Authority (HKMA) published guidance on its supervisory expectations with respect to the adoption of cloud computing. ³¹ In Hong Kong, like in the rest of the world, there has been a growing trend of authorised institutions adopting cloud computing via the engagement of third-party cloud service providers. The HKMA supervisory policy has all along permitted authorised institutions to utilise the technology as long as the associated risks are effectively managed, in compliance with the existing supervisory requirements, including those related to technology risk management and outsourcing. The HKMA noted that, given the growing trend of adoption, and considering that cloud computing does present specific risks, the HKMA considered it appropriate to set out its supervisory expectations on this area in a holistic manner.
IOSCO		In October 2021, the IOSCO published an updated set of outsourcing principles to ensure operational resilience. ³² The Principles on Outsourcing are based on the earlier Outsourcing Principles for Market Intermediaries and for Markets, but have been updated in light of new developments in markets and technology, such as the use of clouds, ICT, data localisation and recent operational events such as COVID-19. The principles apply to trading venues, intermediaries, market participants acting on a proprietary basis and credit rating agencies. While FMIs are outside of the scope of these Principles, FMIs may consider applying the Principles.
Singapore		<p>The Monetary Authority of Singapore (MAS) considers cloud services operated by service providers as a form of outsourcing and has no objections to financial institutions adopting cloud services. MAS published guidelines on outsourcing³³ which set out its expectations of a financial institution that has an outsourcing arrangement in place or is planning to outsource its business activities to a service provider. The guidelines cover engagement with MAS on outsourcing, sound practices on risk management of outsourcing arrangements and cloud computing.</p> <p>Outsourcing outside of Singapore: The engagement of a service provider in a foreign country or an outsourcing arrangement whereby the outsourced function is performed in a foreign country may expose an institution to country risk as well as economic, social and political conditions and events in a foreign country that may adversely affect the institution. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the institution. In its risk management of such outsourcing arrangements, an institution should take into account, as part of its due diligence and on a continuous basis, the following:</p> <ul style="list-style-type: none"> • government policies;

³¹See Hong Kon Guidance on Cloud Computing: [Guidance on Cloud Computing](#)

³²See FSB Enhancing Third-Party Risk Management and Oversight: [Enhancing Third-Party Risk Management and Oversight](#)

³³See MAS Guidelines on Outsourcing: [Guidelines on Outsourcing](#)

		<ul style="list-style-type: none"> political, social and economic conditions; legal and regulatory developments in the foreign country; and the institution's ability to effectively monitor the service provider and execute its business continuity management plans and exit strategy. <p>Material outsourcing arrangements with service providers located outside of Singapore should be conducted in a manner so as not to hinder MAS' efforts to supervise the Singapore business activities of the institution (i.e. from its books, accounts and documents) in a timely manner.</p>
South Africa		<p>The Prudential Authority (PA) issued a directive for cloud computing and data offshoring in South Africa³⁴ for all banks, controlling companies, branches of foreign institutions and auditors of banks or controlling companies. Banks are allowed to use cloud computing and to offshore data as long as they remain in compliance with the relevant requirements specified by the PA as well as other regulatory and supervisory authorities as set out in applicable laws. The ultimate responsibility for managing the risk surrounding cloud computing and data offshoring vests with the relevant bank's Board of Directors (Board). The PA expects banks to follow a risk-based approach aligned with the bank's risk appetite based on the nature and size of its operations when implementing cloud computing and data offshoring.</p> <p>Requests for utilising offshoring and cloud computing for authorised dealers and authorised dealers in foreign exchange (FX) with limited authority will only be considered on a case-by-case basis upon submitting a formal application to the Financial Surveillance Department³⁵ (FinSurv) of the SARB. FinSurv's policy in this regard is outlined under section J.(D) of the Currency and Exchanges Manual for Authorised Dealers as well as section C.1(D) of the Currency and Exchanges Manual for Authorised Dealers in Foreign Exchange with Limited Authority.</p> <p>In April 2021, the Minister of Communications and Digital Technologies published the proposed National Data and Cloud Policy³⁶ in terms of section 3(5) of the Electronic Communications Act 36 of 2005 for comment. The policy applies to all three levels of government (national, provincial and local), organs of state/public enterprises, the private sector and the general public/individual citizens. The policy seeks to create an enabling environment for the provision of data and cloud services to ensure socio-economic development for inclusivity. The objectives of the policy are to:</p> <ol style="list-style-type: none"> 1. Promote connectivity and access to data and cloud services. 2. Remove regulatory barriers and enable competition.

³⁴ See SARB Cloud computing and the offshoring of data: [Cloud computing and the offshoring of data](#)

³⁵ See SARB Offshoring and cloud computing: [Offshoring and cloud computing](#)


³⁶ See DCDT Draft National Policy on data and cloud: [Draft National Policy](#)

		<ol style="list-style-type: none"> 3. Ensure the implementation of effective cybersecurity privacy as well as data and cloud infrastructure protection measures. 4. Provide for institutional mechanisms for the governance of data and cloud services. 5. Support the development of small, medium and micro enterprises (SMMEs). 6. Provide for research, innovation and human capital development. <p>Furthermore, the paper proposed that all data classified/identified as critical information infrastructure be processed and stored within the borders of South Africa. The cross-border transfer of citizen data shall only be carried out in adherence with South African privacy protection policies and legislation (such as the POPI Act)³⁷, the provisions of the Constitution, and in compliance with international best practice.</p> <p>In May 2024 the Minister of Communications and Digital Technologies published the final National Data and Cloud Policy³⁸. The National Data and Cloud Policy is a framework aimed at efficiently managing and utilizing data through cloud computing technologies. Its primary goals are to enhance government service delivery and foster socio-economic development by promoting data-driven decision-making and creating data-based tradable goods and services, thereby supporting an emerging digital economy. Key principles of the policy include:</p> <ol style="list-style-type: none"> 1.1 Accelerating the rollout of digital infrastructure to ensure fast, secure, and reliable broadband connectivity. 1.2 Ensuring data privacy and security. 1.3 Promoting open data and data interoperability. 1.4 Adopting a cloud-first approach. <p>The policy also underscores the importance of capacity building and skills development to encourage the adoption of cloud technologies and data management practices across all sectors. It aims to create a robust data economy that contributes to the growth of the ICT sector and the overall economy.</p> <p>The Policy is also informed by a broad spectrum of legislation, policies, procedures, guidelines, and other documents related to data and cloud computing, including:</p> <ul style="list-style-type: none"> • Protection of Information Act No. 84 of 1982 • Minimum Information Security Standards, 1996 • National Archives and Records Service of South Africa Act, Act No. 43 of 1996 • Promotion of Access to Information Act, Act No. 2 of 2000
--	--	---

³⁷ See SA Government Protection of Personal Information Act 4 of 2013: [Protection of Personal Information Act 4 of 2013](#)

³⁸ See DCDT Draft National Policy on data and cloud: [Draft National Policy](#)

		<ul style="list-style-type: none"> • Electronic Communications Act, Act No. 36 of 2005 • Electronic Communications and Transactions Act No. 25 of 2002 • Spatial Data Infrastructure Act, Act No. 54 of 2003 • National Cybersecurity Policy Framework, 2012 • Protection of Personal Information Act, Act No. 4 of 2013 • Public Administration Management Act, Act No. 11 of 2014 • National Integrated ICT Policy White Paper, 2016 • National e-Strategy, 2017 • Cybercrimes Act, 2020 (Act 19 of 2020) • The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 and • Determination and Directive on the Usage of Cloud Computing Services in the Public Service <p>The policy applies to: National and Provincial government, Organs of State/Public Enterprises, Private Sector, General public/individual citizens, Data Controllers and Data Custodians.</p> <p>Cross-Border Data Transfers and Data Sovereignty: cross-border data transfers and sharing should be carried out in such a manner as to respect the security and sovereignty of South Africa. Policy Interventions:</p> <ul style="list-style-type: none"> • The processing of data collected within the borders of South Africa shall comply with South African data protection and security laws and policies. • Government data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa. • The government shall pursue cross-border data transfers and sharing agreements that meet the following criteria: <ol style="list-style-type: none"> 1. Agreements must promote national interests, including socio-economic development, security, and sovereignty. 2. Agreements must comply with the data protection and data security laws and policies of South Africa. 3. Agreements should enhance mutually beneficial cooperation for all parties involved. 4. Agreements should give effect to the African Continental Free Trade Area (AfCFTA), Southern African Customs Union, Single Digital African Market, and AU and SADC protocols. <p>Policy proposal: the processing of national data, including cross-border data-sharing, shall comply with South African data protection and security laws and policies.</p>
--	--	---


United Kingdom (UK)		<p>In 2016, the Financial Conduct Authority (FCA) published the final version of its guidance paper for firms seeking to outsource functions to the cloud.³⁹ In 2021, the Bank of England (BoE), in a letter⁴⁰ to the industry, outlined the BoE's existing supervisory expectations in relation to material outsourcing arrangements, including the use of public clouds, as they apply to Recognised Payment System Operators (RPSOs) and Specified Service Providers (SSPs). Although the BoE and the FCA had recently strengthened their regulation of the United Kingdom (UK) financial institutions' operational resilience, the increasing reliance on a small number of cloud service providers and other critical third parties for vital services could increase financial stability risk in the absence of greater direct regulatory oversight of the resilience of the services they provide. RPSOs and SSPs' reliance on third parties, in particular through outsourcing arrangements, is well established, and is already subject to existing guidelines set out in the CPMI-IOSCO's PFMI, with which the BoE expects RPSOs to have regard, while SSPs are expected to have regard to Annex F of the PFMI. These requirements also apply when RPSOs and SSPs wish to outsource to a public cloud. RPSOs and SSPs should also have due regard to the BoE's recently published policy on operational resilience⁴¹ and consider any relevant international standards.</p> <p>The BoE expects RPSOs and SSPs to seek its non-objection if they are proposing a change to their business that could materially alter their business model or risk profile. The BoE expects RPSOs and SSPs to notify the BoE and seek its non-objection when there could be a material change in their risk profile and that of the payments ecosystem as a result of participants considering outsourcing their connectivity gateway and/or security solutions that are used to access their services to a public cloud.</p> <p>In 2022, the BoE published a consultation paper⁴² for comments on its proposals around outsourcing and third-party risk management in FMIs. These proposals are set out in three draft supervisory statements for central counterparties (CCPs), central securities depositaries (CSDs), RPSOs and SSPs. They aim to:</p> <ol style="list-style-type: none"> 1. facilitate greater resilience and adoption of the cloud and other new technologies as set out in the BoE's response to the Future of Finance Report; 2. set out the BoE's requirements and expectations in relation to outsourcing and third-party risk management in FMIs; and 3. complement the BoE's supervisory statements on FMI operational resilience.
---------------------	---	--

³⁹ See PRA note Outsourcing functions to the Cloud: [PRA Outsourcing Functions to the Cloud July 2016](#)

⁴⁰ See BOE Supervisory expectations in relation to material outsourcing to the public cloud: [Supervisory expectations](#)

⁴¹ See BOE policy on Operational Resilience of FMIs : [Policy on Operational Resilience of FMIs](#)

⁴² See BOE Outsourcing and third party risk management: Recognised Payment System Operators and Specified Service Providers [Outsourcing and third party risk management](#)

		<p>In 2023, the BoE published outsourcing and third-party risk management policy for FMIs to:</p> <ul style="list-style-type: none"> • facilitate greater resilience and adoption of the cloud and other new technologies as set out in the BoE's response to the Future of Finance report⁴³; • set out the BoE's requirements and expectations in relation to outsourcing and third-party risk management in FMIs; and • complement the BoE's Supervisory Statements on FMI operational resilience. <p>The BoE policy has been issued in the form of Supervisory Statements⁴⁴ for CCPs⁴⁵s, CSDs⁴⁶ and RPSOs & SSPs⁴⁷ and they set out the BoE's requirements and expectations relating to FMIs' outsourcing and third-party risk management. The BoE also issued an outsourcing and third-party risk management part to be added to the Code of Practice applying to relevant RPSOs and SSPs⁴⁸.</p>
United States of America (USA)		<p>According to Bryan Cave Leighton Paisner LLP⁴⁹, in the US, a cloud-computing services contract is largely treated, from a legal perspective, like any other service or commercial contract. Accordingly, cloud-computing services contracts are, in the main, governed by state (and not federal) law, with some federal overlay based on the subject matter of the specific contract.⁵⁰ These include the Gramm-Leach-Bliley Act, which applies to financial services.</p> <p>Federal and state laws and regulations that apply generally to third-party service providers in given industries, such as:</p> <ul style="list-style-type: none"> • third-party risk guidance for the financial services industry from the US Federal Reserve (Fed); • the Financial Industry Regulatory Authority (FINRA); • the Office of the Comptroller of the Currency (OCC); and • the New York State Department of Financial Services (NYSDFS). <p>According to the FSB⁵¹, the US tends to issue principles-based regulations and supplement them with guidance in, for instance, circulars, letters and explanations of supervisory practices.</p>

⁴³See BOE: [The Future of Finance - our response | Bank of England](#)

⁴⁴See FMI Outsourcing and Third Party Risk Management Policy Statement: [Policy Statement](#)

⁴⁵See Outsourcing and Third Party Risk Management Statement: [Outsourcing and third party risk management Supervisory Statement](#)

⁴⁶See BOE Outsourcing and third party risk management Supervisory Statement: central securities depositories: [Outsourcing and third party risk management](#)

⁴⁷See BOE Outsourcing and third party risk management Supervisory Statement: recognised payment system operators and specified service providers: [Outsourcing and third party risk management](#)

⁴⁸See BOE Outsourcing and third party risk management Supervisory Statement: recognised payment system operators and specified service providers: [Outsourcing and third party risk management](#)

⁴⁹See Lexology Cloud computing law in USA: [Cloud computing law in USA](#)

⁵⁰See FSB Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: [Discussion paper](#)

⁵¹ See FSB Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: [Discussion paper](#)

		<p>In addition, certain US agencies also have the legal authority to directly supervise specific services provided to banks by third-party providers. Their supervisory authority is nevertheless limited to the services being provided to deposit-taking institutions rather than the full oversight or supervision of the third-party entities providing the services.</p> <p>According to Bryan Cave Leighton Paisner LLP⁵², data security and protection requirements at the state level vary significantly, with breach notification laws in all 50 states and some of the more protective privacy regimes existing under the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, the New York SHIELD Act and the NYSDFS cybersecurity regulations.</p> <p>Finally, US customers with international operations remain subject to international privacy laws like the EU's GDPR.</p> <p>In addition to the data privacy regulations, there is third-party risk guidance from the Fed, the OCC, FINRA, the NYSDFS and other regulatory agencies that may apply to the use of cloud computing in the financial services industry, and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) permits federal authorities to compel US-based companies to provide access to data that may be stored on servers in the US and other jurisdictions. It will also indirectly impact on cloud computing, including the offshore storage of data.</p>
--	--	---

⁵² See Lexology Cloud computing law in USA: [Cloud computing law in USA](#)

9. Policy and regulatory recommendations for the use and adoption of cloud computing and data offshoring in the NPS

9.1 **Policy recommendation:** This consultation paper also seeks to ensure that the adoption of cloud computing and data offshoring by payment institutions and operators is focused on supporting the following objectives aligned to the SARB's mandate and the goals of the National Payment System Framework and Strategy (*Vision 2025*):

9.1.1 **Safety, efficiency, stability and integrity of the NPS:** The adoption of cloud computing and data offshoring in the NPS must be implemented with a robust risk and governance framework that places a high priority on the safety, efficiency, stability and integrity of payment institutions, operators and the NPS. The risk associated with the adoption of cloud computing and data offshoring, discussed in this consultation paper, might lead to disruptions to payment institutions, operators, the NPS and the broader financial system, and might undermine public confidence in the safety, efficiency, stability, integrity and reliability of the NPS.

9.1.2 **A clear and transparent regulatory and governance framework:** This consultation paper seeks to develop a clear and transparent regulatory framework for using cloud computing and data offshoring for all the payment institutions and operators in the NPS. To ensure stability and safety within payment systems, all payment institutions and operators should be subject to clear and transparent regulation and governance frameworks for adopting cloud computing and data offshoring in a manner appropriate and proportionate to the risk introduced into the NPS through such practices.

9.1.3 **Financial stability and security:** The stability and security of the NPS is of paramount importance for the SARB and all other payment system stakeholders. The adoption of cloud computing and data offshoring can improve cyber-resilience in the NPS, thus improving security – and with

enhanced security, there is less likelihood of disruptions that might lead to adverse impacts on financial stability. Increased security and resilience are some of the advantages of cloud computing and data offshoring, as they can also be more secure and resilient than traditional platforms and data centres, with major cloud service providers often being at the forefront of security implementation and research. Payment institutions and operators typically have legacy infrastructures and data centres that are more exposed to cyber-threats and cyberattacks.

9.1.4 Promoting competition and innovation: The SARB supports efforts to increase competition in specific layers of the payment services value chain to foster the development of innovative services while continuing to ensure the safety and efficiency of the NPS. The traditional payment landscape operates with complexity and expensive data centres and infrastructures. Large payment institutions and operators continually invest in new and advanced infrastructure to ensure smooth operations. Cloud computing and data offshoring enables payment institutions and operators to benefit from economies of scale inherent in sharing the vast resources of the cloud service providers in various jurisdictions. Payment institutions and operators can automatically scale up when additional resources are needed and scale down when demand decreases.

9.1.5 Cost-effectiveness: The adoption of cloud computing and data offshoring contributes to lower technology infrastructure costs, transforming large upfront capital expenditures into smaller ongoing operational costs. Payment institutions and operators benefit from lower costs for purchasing, supporting and maintaining technology infrastructure and data centres. A cloud's scalability allows payment institutions and operators to test new payment services and products, software tools and alternative configurations without a lengthy purchasing and provisioning process of ICT infrastructures and data centres.

9.2 Regulatory recommendations: The SARB should enable payment institutions and operators to use cloud computing and to only offshore non-

critical payment data and processes as long as such payment institutions and operators remain in compliance with the relevant requirements specified by the SARB and other regulators and supervisory authorities as set out in applicable laws and regulatory frameworks. Payment institutions and operators must obtain the approval of the SARB prior to cloud utilisation and data offshoring. However, clearing and settlement data and systems for payment system FMs must be processed, stored and/or located within the borders of South Africa. The adoption and use of cloud computing for payment system FMs should be limited to onshore cloud services. Clearing and settlement is critical to the NPS and the financial system and should be retained within the borders of South Africa. To maintain the safety, integrity and efficiency of the NPS, the SARB should impose the following regulatory requirements in the form of a directive in terms of section 12 of the NPS Act to regulate the use of cloud computing, cloud-computing service providers and data offshoring in the NPS.

9.3 Requirements for the adoption of cloud computing and data offshoring for payment system FMs

9.3.1 Clearing and settlement services and activities offered by PCH SOs and RTGS operators

- a. Clearing and settlement services and activities, data, mechanisms, processes, infrastructures and systems are critical to the NPS and the financial system and should be retained within the borders of South Africa. Designated settlement systems for cross-border payments, such as SADC's real-time gross settlement (RTGS) system and the Continuous Linked Settlement (CLS) system, are excluded from this requirement.
- b. The offshoring of clearing and settlement services and activities, data, mechanisms, processes, infrastructures and systems should be prohibited

for PCH SOs and RTGS operators as payment system FMIs.⁵³ Designated settlement systems for cross-border payments, such as SADC's RTGS system and the CLS system, are excluded from this requirement.

- c. The cloud computing services, and infrastructure should be located and retained within the borders of South Africa for clearing and settlement services and activities, data, mechanisms, processes, infrastructures and systems by PCH SOs and RTGS operators as payment system FMIs. Designated settlement systems for cross-border payments, such as SADC's RTGS system and the CLS system, are excluded from this requirement.
- d. The adoption of cloud computing as well as the use of cloud-computing service providers and other offshore service providers by PCH SOs and RTGS operators as payment system FMIs should be in accordance with the PFMI, including Annex F on the oversight expectations applicable to critical service providers and supporting guidance on FMIs issued by the CPMI and IOSCO.
- e. Payment system FMIs that are PCH SOs and RTGS operators should ensure that their cloud service provider or other offshore service provider complies with Annex F of the PFMI. Annex F sets out the expectations aimed at critical service providers; it also covers risk identification and management, information security, reliability and resilience, technology planning and user communication. Payment system FMIs remain ultimately responsible for its operations.

9.3.2 **PCH SOs' entry and participation criteria**

- a. The adoption of cloud computing as well as the use of cloud-computing service providers and other service providers by PCH SOs should comply with the PCH SOs' entry and participation requirements, and should ensure

⁵³ According to the PCH SO criteria, value-added services such as tokenisation are excluded, and settlement activities of PCH SOs may take place outside of South Africa.

that the clearing services rendered in respect of domestic transactions as well as the services pertaining to transaction authorisation are rendered through the infrastructure, including cloud infrastructure where applicable, that is established and maintained in South Africa. In addition, clearing and authorisation data should be stored, and records should be retained in South Africa.

9.4 Requirements for the adoption of cloud computing and offshoring of non-critical payment data and processes for all payment institutions and operators

9.4.1 Operational capability

- a. The offshoring of non-critical payment data and processes by payment institutions that are not FMIs, the adoption of cloud computing and the use of cloud-computing service providers and other offshore service providers must not result in the payment institution becoming a shell company without the necessary operational capability to perform its authorised, registered or licensed functions or activities, or to provide payment, clearing and settlement services.
- b. Payment system FMIs must ensure the adoption of cloud computing, and the use of cloud-computing service providers limited to onshore must not result in the payment system FMIs becoming a shell company without the necessary operational capability to perform its authorised, registered or licensed functions or activities, or to provide payment, clearing and settlement services.

9.4.2 Regulatory, supervisory and oversight obligations

- a. Payment institutions and operators, including payment system FMIs, must retain full responsibility and accountability relating to their compliance with regulatory, supervisory and oversight requirements, and may not delegate accountability to the cloud service provider or other offshore service

provider. This includes compliance with the NPS Act, all the regulatory instruments issued in terms of the NPS Act, other financial sector laws, the PFMI (including Annex F) and supporting guidance on FMIs issued by the CPMI and IOSCO.

- b. The SARB must be able to effectively regulate, oversee and supervise all payment institutions and operators, including the payment activities, systems, data and operations migrated on the cloud, other offshore service providers or an offshore parent organisation.
- c. The SARB must have a comprehensive overview of the payment services, data activities, infrastructures, systems and operations to be migrated on the cloud or offshoring of non-critical services (for payment institutions that are not payment system FMIs) and the arrangements between cloud service providers, other offshore service providers or their offshore parent organisation, including all possible risks. All payment institutions and operators must provide the following information to the SARB prior to migration to the cloud or data offshoring for consideration and approval:
 - i. a brief description of the payment activities, services, data, mechanisms, processes, infrastructures and systems to be migrated to the cloud or offshored;
 - ii. a brief description of the non-critical payment data and processes to be offshored as well as a detailed description of the non-critical payment data and processes;
 - iii. the following details of the cloud service provider offshore service provider or offshore parent organisation:
 - details of the legal person, including certified copies of the notice of incorporation and registration certificate issued by the Companies and Intellectual Property Commission (CIPC) under the Companies Act 71 of 2008 (Companies Act) or an equivalent body;

- a certified copy of the memorandum of incorporation lodged with the CIPC or an equivalent body;
 - the address of the cloud service provider, offshore service provider or offshore parent organisation's place of business;
 - the agreements/contracts between the payment institution and cloud service provider; and
 - any other details requested by the SARB;
- iv. the details of the cloud service, service provider and deployment models, for example whether they are public, private, hybrid or community, as well as the specific nature of the non-critical data and processes to be held and the countries where such data will be stored and processed;
- v. whether or not the payment activities, services, data, mechanisms, processes, infrastructures and systems to be hosted on the cloud are considered critical or important, and a motivation for the response provided; and
- vi. whether or not the cloud service provider or service provider will outsource any of its critical operations to another fourth-party provider and how fourth-party risk will be mitigated.
- d. All payment institutions and operators must adequately inform the SARB in a timely manner about their intentions to migrate payment activities, services, data, mechanisms, processes, infrastructures and systems to a cloud and the use of cloud service providers. Payment institutions and operators that are not payment system FMIs must adequately inform the SARB in a timely manner about their intentions to offshore any non-critical payment data and processes to a cloud service provider, another offshore service provider or an offshore parent organisation.

- e. Payment institutions and operators must adequately inform the SARB in a timely manner of any material changes and adverse developments arising from the adoption and use of cloud computing and cloud-computing service providers as well as the offshoring of non-critical payment data and processes that could have a material impact on the continuing provision of the payment institution's payment services and activities as well as an impact on the safety and efficiency of the NPS. Such adverse developments include any event that could potentially lead to prolonged service failure or disruption, or any breach of security and confidentiality of the payment institution and operators payment data, information and operations.
- f. The SARB may require a payment institution and operators to modify, make alternative arrangements or re-integrate a payment service, activity, data, mechanisms, processes, infrastructures and systems migrated to the cloud into the payment institution and operators in the event of non-compliance with the legal, regulatory and supervisory framework to mitigate the risk of the adoption of cloud computing and cloud-computing service providers in the NPS. In addition, the SARB may require a payment institution and operators to modify, make alternative arrangements or re-integrate offshored non-critical payments data and processes from a service provider or offshore parent organisation into the payment institution and operators in the event of non-compliance with the legal, regulatory and supervisory framework to mitigate the risk of offshoring non-critical payments data and process services in the NPS. This includes, for example, if:
 - i. A payment institution and operators cannot demonstrate an in-depth understanding of the nature and extent of risk arising from the use of cloud computing and cloud-computing service providers for payment services, activities, systems, data and operations in the NPS.
 - ii. A payment institution and operators that is not a payment system FMI cannot demonstrate an in-depth understanding of the nature and extent of risk arising from the offshoring of non-critical payment data

and processes to a service provider or offshore parent organisation for the payment data and processes in the NPS.

- iii. A payment institution and operators cannot adequately implement a risk management framework to identify, assess, report, monitor, manage and mitigate the risks associated with the use of cloud computing and reliance on cloud-computing service providers in a satisfactory and timely manner.
- iv. A payment institution and operators that is not a payment system FMI cannot adequately implement a risk management framework to identify, assess, report, monitor, manage and mitigate the risks associated with offshoring non-critical payment data and processes to a service provider or offshore parent organisation in a satisfactory and timely manner.
- v. The safety, security, confidentiality and protection of the payment institution and operator's data and information are decreased due to changes in the control environment of the cloud service provider, a service provider or its offshore parent organisation.
- vi. The SARB's regulatory, supervisory and oversight powers and functions over the payment institution and operators are impeded by the migration of payment services, activities, data and operations on the cloud as well as the use of cloud service providers and/or offshoring of non-critical payment data and processes to a service provider or offshore parent organisation.

9.4.3 Cloud location

- a. With the use of cloud computing and cloud-computing service providers, payment institutions and operators that are payment system FMIs should ensure the cloud is located in South Africa. Designated settlement systems

for cross-border payments, such as SADC's RTGS system and the CLS system, are excluded from this requirement.

- b. Payment institutions and operators that are payment system FMIs should ensure that the cloud infrastructure used for clearing and settlement activities, services, data, mechanisms, processes, infrastructures and systems is located in South Africa. Designated settlement systems for cross-border payments, such as SADC's RTGS system and the CLS system, are excluded from this requirement.
- c. The use of cloud computing and cloud-computing service providers by payment institutions and operators that are not payment system FMIs for critical payment data and processes should ensure that the cloud is located in South Africa.
- d. Payment institutions and operators that are not payment system FMIs are allowed to offshore non-critical payment data and processes to the cloud and cloud service providers, other offshore service providers and offshore parent organisations. The highest risk in cloud computing involves geopolitical tensions. This includes potential compromises in the host country of the data or directives to cloud providers based on their domicile legislation. Given the dominance of US and Chinese cloud providers, South African entities should mitigate risks by either maintaining minimum essential loads/copies within South Africa or diversifying our cloud provider portfolio to include both Eastern and Western companies.

9.4.4 **Data protection**

- a. The public has confidence in payment institutions, operators and the NPS due to the safety and efficiency of payment systems in South Africa. A payment institution and operators must satisfy itself that the cloud service provider, other offshore service provider or offshore parent organisation's security policies, procedures and controls will enable it to protect the

confidentiality, integrity, safety and security of payment data, information and operations in the NPS.

- b. The performance and quality of the cloud service provider or offshore service provider as well as the level of operational risk that they may cause to the payment institution and operators are primarily determined by the ability of the cloud service provider or offshore service provider to appropriately protect the confidentiality, integrity and availability of data (in transit or at rest) and the ability of the systems and processes that are used to process, transfer or store such data. Appropriate traceability mechanisms aimed at keeping records of technical and business operations are also vital in detecting malicious attempts to breach the security of data and systems. Security expectations should take into account the need to protect the data and systems.
- c. The payment institution and operators should carry out a security risk assessment and should have appropriate protection and confidentiality arrangements in place for the protection and integrity of data, information, systems and processes shared between the payment institution, operators and the cloud service provider, offshore service provider or offshore parent organisation, and this should be in accordance with the POPI Act.
- d. Payment institutions and operators should monitor, on an ongoing basis, the performance of the service providers regarding the availability, integrity and security of data and information transmitted and stored on the cloud with the cloud service provider, offshore service provider or offshore parent organisation. Payment institutions and operators should consider how data will be segregated (if using a public cloud), take appropriate steps to mitigate security risks, and consider data sensitivity and how the data is transmitted, stored and encrypted, where necessary, with the cloud service provider, service provider or offshore parent organisation.
- e. The payment institution and operators should ensure that the cloud service provider, offshore service provider or onshore parent organisation complies

with applicable domestic and international standards and practices for IT security standards, data and information security management systems for cyber-protection as well as data protection. Where relevant, the payment institution and operators should define data and system security requirements within the cloud service agreement and should monitor compliance with these requirements on an ongoing basis.

9.4.5 Robust governance and risk management framework and arrangements

- a. Payment institutions and operators must have a robust governance framework and arrangements in place, approved by the Board or senior management, for using cloud computing, cloud-computing service providers, offshore service providers and offshore parent organisations. The governance arrangements should focus on supporting the safety, efficiency, integrity and objectives of the NPS.
- b. Payment institutions and operators must have robust policies, procedures and due diligence checks in place for selecting and substituting a cloud service provider, offshore service provider or offshore parent organisation.
- c. Payment institutions and operators must consider the relative risks of using one type of cloud service over another (e.g. public versus private cloud) and should use more than one cloud service provider to minimise the concentration risk.
- d. Payment institutions and operators should ensure that cloud service providers, offshore service providers or offshore parent organisations have robust cyber-resilience measures in place that are regularly monitored and tested against evolving cyber-threats and must comply with the regulatory requirements on cybersecurity.

- e. The Board and senior management of the payment institution and operators should ensure a sound risk management culture and environment for using cloud computing, cloud-computing service providers and data offshoring.
- f. The Board and senior management of the payment institution and operators should ensure that there are adequate processes in place to provide a comprehensive institution-wide view of the payment institution and operator's risk exposures from cloud computing, cloud-computing service providers, offshore service providers or offshore parent organisations, and should incorporate the assessment and mitigation of such risks into the payment institution's risk management framework.
- g. Payment institutions and operators must have measures in place for implementing, monitoring and managing cloud service providers and offshoring non-critical payment data and processes, including the ongoing assessment of the service provider's performance to deliver what is required by the payment institutions, operators and BCP.
- h. Payment institutions and operators must have appropriate BCP in place to ensure that they can continue functioning and meeting their regulatory, supervisory and oversight obligations in case of an unforeseen interruption of cloud services, service providers or offshore parent organisations. Such BCP should also take into account the potential impact of the insolvency or other failures of the cloud service provider or service provider and, where relevant, political risks in the service provider's jurisdiction. Payment institutions and operators should have in place, maintain and periodically test appropriate BCP with the cloud service provider, offshore service provider or offshore parent organisation. BCP should be aligned with the BCP requirements set by the payment system management body, RTGS operators' service level agreements and PFMI for payment system FMIs.
- i. Payment institutions and operators must have exit strategies and termination processes in place for cloud computing or service provider arrangements. These strategies and termination procedures must be

understood, documented, fully tested and aligned with the payment institution's regulatory, supervisory and oversight requirements. Such exit strategies and termination processes should consider possible service interruptions or the unexpected termination of the agreement with a cloud service provider or service provider. Payment institutions and operators should ensure that they can exit arrangements with a cloud service provider or service provider without undue disruption to their payment activities, services, data, mechanism, processes, infrastructures and systems; without limiting their compliance with regulatory, oversight and supervisory requirements; and without any detriment to the continuity and quality of their provision of payment services and products to their customers in the NPS.

9.4.6 Adequate risk management framework

- a. Payment institutions and operators must have an appropriate, adequate and documented risk management framework in place to identify, assess, report, monitor, manage and mitigate the risks associated with the use of cloud computing as well as the offshoring of non-critical payments data and processes to a service provider or offshore parent organisation, and reliance on cloud-computing service providers or service providers.
- b. These risks include, among other things, operational, reputational, concentration, systemic, vendor lock-in, third-party dependency, subcontractors located in other jurisdictions, political instability and the security situation of the jurisdictions where the cloud service provider, offshore service provider or offshore parent organisation is located or the subcontractor and their legal framework, data privacy and cybersecurity risks, including exposure to the shortage of relevant resources and ICT skills within the regulated entity.
- c. The risk assessment in the risk framework must include, where appropriate, scenarios of possible risk events, including high-severity operational risk events. Within the scenario analysis, payment institutions should assess

the potential impact of failed or inadequate services, including the risks caused by processes, systems, people or external events.

9.4.7 Recovery or orderly wind-down and/or resolution

- a. Payment institutions and operators, especially payment system FMIs, must ensure that their cloud arrangements and offshoring of non-critical payment data and processes will not compromise compliance with the recovery, orderly wind-down or resolution standards issued by the SARB. If a payment institution and operators, especially an FMI, decides to use cloud computing and cloud-computing service providers, the payment institution must consider its recovery or orderly wind-down planning and resolution planning. The operational continuity of critical functions must be ensured even when in financial distress or during financial restructuring or resolution. The decision to migrate to the cloud and to use cloud service providers should not in any way impede the recovery, orderly wind-down or resolution of the payment institution, or create additional complexity to this process.

10. Questionnaire

- 10.1 Stakeholders and other interested parties are encouraged to respond to the questions below using the SARB template as part of the consultation feedback to the SARB:
 - 10.1.1 Is your institution using cloud computing for payments in the NPS? Please provide the SARB with the details of your cloud-computing service provider and model.
 - 10.1.2 Has your institution offshored payment data and processes in the NPS? Please provide the SARB with the details of the offshored payment data and processes in the NPS.

- 10.1.3 What are the use cases for cloud computing in the NPS?
- 10.1.4 What are the use cases for data offshoring in the NPS?
- 10.1.5 Please provide the SARB with a list of the payment activities, services, data, mechanisms, processes, infrastructures and systems migrated to the cloud by your institution or the intention to do so. Are the payment activities, services, data, mechanisms, processes, infrastructures and systems critical
- 10.1.6 Please provide the SARB with the details of the cloud service provider, offshore service provider or offshore parent organisation used by your institution.
- 10.1.7 Please indicate whether or not the payment activities, services, data, mechanisms, processes, infrastructures and systems hosted on the cloud are considered critical and provide motivation for the response provided.
- 10.1.8 What other benefits of cloud computing should be mentioned in the consultation paper?
- 10.1.9 What other benefits of data offshoring should be mentioned in the consultation paper?
- 10.1.10 What other risks associated with cloud computing should be mentioned in the consultation paper?
- 10.1.11 What other risks associated with data offshoring should be mentioned in the consultation paper?
- 10.1.12 How does your institution mitigate the risks associated with cloud computing?
- 10.1.13 How does your institution mitigate the risks associated with data offshoring?
- 10.1.14 What are your institution's views on cloud computing, data offshoring and cybersecurity risk?

- 10.1.15 How does your institution mitigate risks associated with cloud computing, including but not limited to service outages, vendor lock-in, as data breaches, supervisory and regulatory requirements?
- 10.1.16 How does your institution address risks associated with data offshoring, such as cross-border data access, data protection etc?
- 10.1.17 What are your institution's views on the definition of a critical payment data, processes, activities and service in the policy paper.
- 10.1.18 How does your institution determine critical payment data, processes, activities and service? Please include examples.
- 10.1.19 How does your institution determine non-critical payment data, processes, activities and service? Please include examples.
- 10.1.20 How does your institution assess the interdependencies between critical and non-critical payment activities, systems, and data?
- 10.1.21 What other policy and regulatory recommendations for the use and adoption of cloud computing and data offshoring in the NPS should be mentioned in the consultation paper?

11. Conclusion

- 11.1 The demand for computational resources will continue to expand rapidly. It is driven by the increasing interest in Big Data, new analytical methods in data science and technological progress. Therefore, cloud computing and data offshoring will continue to be a popular solution for payment institutions to meet their computational needs. In its regulatory, supervisory and oversight capacity, the SARB will continue to play an essential role in ensuring that the adoption and use of cloud computing and data offshoring is aligned with the safety and efficiency of the NPS.

12. Comments, consultation questions and contact details

- 12.1 Stakeholders and other interested parties are invited to send their comments on this consultation paper using the SARB template by **15 May 2025**. Comments should be addressed to npsdirectives@resbank.co.za.

ABBREVIATIONS

BCP	business continuity planning
BIS	Bank for International Settlements
Board	Board of Directors
BoE	Bank of England
BPaaS	business process as a service
CCP	central counterparties
CEBS	Committee of European Banking Supervisors
CIPC	Companies and Intellectual Property Commission
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CLS	Continuous Linked Settlement
CMA	Common Monetary Area
Companies Act	Companies Act 71 of 2008
CPMI	Committee on Payments and Market Infrastructures
CSD	central securities depositaries
DCDT	Department of Communications and Digital Technologies
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EIOPA	Occupational Pensions Authority
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
Fed	Federal Reserve
FINRA	Financial Industry Regulatory Authority

FinSurv	Financial Surveillance Department
fintech	financial technology
FMI	financial market infrastructure
FSB	Financial Stability Board
FX	foreign exchange
G20	Group of Twenty
GDPR	General Data Protection Regulation
HKMA	Hong Kong Monetary Authority
ICT	information and communication technology
IOSCO	International Organization of Securities Commissions
IT	information technology
IaaS	infrastructure as a service
MAS	Monetary Authority of Singapore
MasterCard	MasterCard Limited
NPS Act	National Payment System Act 78 of 1998, as amended
NPS	national payment system
NPSD	National Payment System Department
NYSDFS	New York State Department of Financial Services
OCC	Office of the Comptroller of the Currency
PA	Prudential Authority
PaaS	platform as a service
PASA	Payments Association of South Africa
PCH SO	payment clearing house system operator
PFMI	Principles for Financial Market Infrastructures

POPI Act	Protection of Personal Information Act
RPSO	Recognised Payment System Operator
RTGS	real-time gross settlement
SaaS	software as a service
SADC	Southern African Development Community
SARB Act	South African Reserve Bank Act 90 of 1989, as amended
SARB	South African Reserve Bank
SMMEs	smalls, medium and micro enterprises
SO	system operator
SRC	Supervisory and Regulatory Cooperation
SSP	specified service providers
UK	United Kingdom
UNCTAD	United Nations Conference on Trade and Development
US	United States
Visa	Visa Limited