12 October 2020

Dr. Reza Baqir
Honourable Governor
The State Bank of Pakistan I.I. Chundrigar Road Karachi, Pakistan

Dear Sir,

Subject: Industry Submission on the BPRD Circular No. 04 of 2020 on Outsourcing to Cloud Service Providers (CSPs)

The Asia Internet Coalition (AIC) would like to take this opportunity to commend the State Bank of Pakistan (SBP) recent decision to allow financial institutions to use cloud services through BPRD Circular No. 04 of 2020 on Outsourcing to Cloud Service Providers. The AIC is an industry association comprised of leading Internet and technology companies and seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our members are Airbnb, Amazon, Apple, Cloudflare, Expedia Group, Facebook, Google, SAP, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com.

First and foremost, we congratulate your leadership and the vision on drafting the Circular which is seen as a progressive and positive step for financial institutions to outsource hosting on the cloud to both domestic and international cloud service providers (CSPs). While, the Circular updates part of the language of two earlier circulars issued in 2017 and 2019, to do with the 'Enterprise Technology Governance and Risk Management Framework for Financial Institutions (FIs)', the underlying decision by SBP will provide access to a much needed FinTech infrastructure in Pakistan. The progressive policy measure, which will empower financial institutions to leverage cloud services to a significant extent, demonstrates the commitment of the SBP towards enhancing the cybersecurity and consumer protection of Pakistan's digital financial ecosystem.

The Circular aims to simplify the government's stance on data sovereignty, which is confused with the concept of data residency. It also emphasizes on the importance of security as one of the objectives in migrating workload and data onto the cloud to mitigate the risks and vulnerabilities associated with their adoption of the chosen cloud deployment model. It also enhances the concept of data ownership, thereby ensuring the transfer, storage, or processing of data in cloud infrastructure. FIs and technology-dependent companies, rely on cloud storage solutions for their data management because it allows an affordable and scalable way to deploy the latest technology and tools across the network to make it secure. This is not possible with data localization.

We hope that similar progressive measures are reflected by the Ministry of Information Technology & Telecommunication (MOITT) against regressive data localization policies, such as those found in the Personal Data Protection Bill (PDP Bill) currently under consideration. Cross-border data flow has become even more critical during the pandemic as governments and medical researchers around the world exchange information and work together to find a vaccine to COVID-19. These exchanges naturally involve cross-border data flows.

Data localization requirements will stifle investment in Pakistan's digital economy and prove harmful to the country's long-term economic growth. The ill-conceived notion of data localization will not only hurt international players but will also impact local businesses in Pakistan, and render the current state of infrastructure vulnerable to cyber threats, as witnessed in several cyber incidents where data was localized thereby undermining resilience, security and accessibility of digital infrastructure. We recognise that the Government of Pakistan has the responsibility to ensure national security and protect its citizens. However, in most instances, data localization mandates do not increase commercial privacy nor data security, as it creates a single-point-of-failure. A report from the Leviathan Security Group[1] shows that data localization measures raise the cost of hosting data by 30-60%. This is because the internet enables centralized data storage and processing, taking advantage of economies of scale and a seamless, global internet. When governments break apart these efficiencies, they exponentially raise the cost of doing business.

We hope that the SBP will, in due time, also consider further merits of cloud services and useful application of cloud computing in regulatory technology and supervisory technology[2]. Enabling FIs to leverage the cloud will improve business operations efficiency and overall security, including the use of artificial intelligence (AI) and big-data analytics to reduce risks and improve resilience. FIs will be able to reap the benefits from greater operational efficiency by enabling better integration of business units through improved data sharing, the use of common data sets, more sophisticated data analytics and ultimately, shared insights.

As responsible stakeholders towards the policy making process, we would like to submit our views and recommendations for SBP's further consideration and express our shared goals of encouraging growth and consumer choice in the digital and financial ecosystem in Pakistan. As such, please find appended to this letter, our comments and recommendations (see Appendix).

1 https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf

2 https://www.esma.europa.eu/press-news/esma-news/regtech-and-suptech-–-change-markets-and-regulators

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)
Jeff@aicasia.org
secretariat@aicasia.org

CC:

1. Mr. Jens Weidmann
   Chairman of the Board Bank for International Settlements

2. Mr. Shoaib Ahmad Siddiqui Secretary IT
   Ministry of Information Technology & Telecommunication

Appendix

Introduction

The AIC welcomes the enhanced scope of outsourcing to Cloud Service Providers (CSPs) for Banks/DFIs/Microfinance Banks (collectively referred to as Financial Institutions or FIs). The FIs will now be able to avail all types of cloud service models including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) etc. from domestic and off-shore CSPs.

Many banks and consumer financing companies are either fully digitized or are digitizing their processes and services. Further, large corporations and financial institutions (both government owned and private) are using global banking services by international FIs. The new Circular will substantially accelerate cloud adoption by FIs that are transforming their businesses and services through new customer offerings.

The circular represents a best practice to not have criteria of preference between domestic CSPs over foreign competitors, thereby creating market entry for varied players, promoting competition and encouraging use of international standards. Global CSPs have the expertise and resources to offer the highest level of data security, reliability and quality of service, often at a lower cost. The Circular acknowledges that the use of cloud services provides business agility and allows FIs to respond to customer needs and achieve economies of scale, and provides an approval mechanism so that FIs are able to enter into outsourcing agreement with CSPs.

The Circular also aims to simplify the government's stance on data sovereignty, which is confused with the concept of data residency. It also emphasizes on the importance of security as one of the objectives in migrating workload and data onto the cloud to mitigate the risks and vulnerabilities associated with their adoption of the chosen cloud deployment model. It enhances the concept of data ownership, thereby ensuring the transfer, storage, or processing of data in cloud infrastructure. FIs and technology-dependent companies, rely on cloud storage solutions for their data management because it allows an affordable and scalable way to deploy the latest technology and tools across the network to make it secure. This is not possible with data localization.

Like the governments of Singapore, Thailand, Malaysia and the Philippines that do not have any data residency restrictions in place, the SBP sets a forward looking example. However, such practices are not reflected in other policies that are under development in Pakistan. For example, we are concerned that certain aspects of the Draft Data Protection Bill 2020 (PDP Bill) – particularly those relating to data localization – will adversely impact Pakistan's digital ambitions. Such requirements will undermine privacy and data security, stifle innovation and growth in technology and internet-dependent industries. SBP emphasizes on the data transferability and portability for data when FIs use cloud outsourcing arrangements. This is a crucial factor that supports data flow that is a key driver of the digital world that we live in. Cross-border data flow has become even more critical during the pandemic as governments and medical researchers around the world exchange information and work together to find a vaccine to COVID-19. All these depend on cross-border data flow.

Data localization provisions contemplated in the PDP bill would make it difficult for Pakistani companies to gain access to innovative technologies like data analytics, artificial intelligence and machine learning tools, etc. that depend on data flows. They may also lose access to cost-efficient cloud services in the global market. All these in turn will negatively impact consumers in Pakistan who will have to pay higher prices and have a limited variety of digital products and services to choose from.

We recommend aligning the PDP Bill to the principles embodied in the Circular to ensure that Pakistan's FIs are able to take advantage of the innovative services and cost-saving features of the cloud, and do not fall behind peers in the region.

Other considerations

1. FIs should be aware of cloud services' typical characteristics such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations. Hence, FIs should take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. In particular, FIs should ensure that the service provider possesses the ability to clearly identify and segregate customer data using strong physical or logical controls. The service provider should have in place robust access controls to protect customer information and such access controls should survive the tenure of the contract of the cloud services.

2. FIs are ultimately responsible and accountable for maintaining oversight of cloud services and managing the risks of adopting cloud services, as in any other form of outsourcing arrangements. A risk-based approach should be taken by FIs to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the cloud services.

3. One of the key benefits of cloud computing is the ability to move workloads efficiently and swiftly as needed in a scalable and an agile environment. Any regulatory approval required for FIs adoption of cloud services will hinder the realization of these benefits. Regulatory approvals can delay deployment, slowing response to business needs and efficient data management. In this regard, a notification to the regulator where a workload is to be migrated to a cloud service should be adequate, wherein a notification could be addressed in review of risk assessment frameworks. SBP should consider CSPs certifications of compliance with global standards and best practices in the context of contracting with an FI, and based on those certifications, approval of the CSP should be applied for use by other FIs. We further recommend integrating the use of a risk assessment framework when FIs engages with CSP. In this case, rather than approval, there could be a requirement to inform the SBP when an FI engages a CSP or moves a new workload to the CSP. Notification to inform will provide the SBP the opportunity to

consider compliance without delaying the deployment unnecessarily (refer to Australia's APRA's framework[3]).

4. Cross border data flow is an essential component in the journey to the cloud. This is consistent with the cross-border nature of financial services, which SBP clearly acknowledges. With no requirements for data to be stored in specific geographies will overcome risk vulnerabilities for the FIs and improve efficiency and benefits from economies of scale that cloud accompanies. Major CSPs operate data centers across the globe, and their resources can serve an FI from several locations, thereby providing better redundancy with the high security standards.

5. A risk based approach to regulatory compliance encourages FIs to implement outsourcing in a way that reflects the nature of risk in, and materiality of, the outsourcing agreements. A risk-based approach encourages innovation, scalability while maintaining an appropriate risk management regime. Refer to the Association of Banks in Singapore (ABS) second version of the implementation guide for FIs when entering into Cloud outsourcing arrangements[4]. The guidance allows an FI to assess the inherent risk profile of a Cloud Outsourcing arrangement, and then ensure that appropriate controls are in place to ensure that residual risks are appropriately managed and monitored and thus remain within appetite.

6. SBP should not create a right to government for unrestricted physical audit access rights to CSP facilities. Physical access to CSP facilities is not necessary for audits or oversight and creates unnecessary security risks to the CSP and its customers. Alternatively, a certified audit conducted on a regular basis with reports made available to SBP can address oversight objectives. The FI should establish an organisational structure and reporting lines for IT audit in a way that preserves the independence and objectivity of the IT audit function. When the audit activity involves a CSP's data centers, there is no need for the regulator to have direct – and absolutely unlimited – access rights to enter the CSP's facilities at will. It is important that the CSP be allowed reasonable control over access to their facilities for the sake of security. Therefore, SBP should recognise that CSPs have regular third-party audits to serve the needs of multiple FI customers.

7. It is recognized that moving technology infrastructure into the cloud creates a shared responsibility model between the consumer and the CSP for the operation and management of security controls. A clear distinction between data controllers and data processors is important for it allows better understanding of the different responsibilities between the entity that has control of data and the entity that processes the data, and ensures there is clarity as to which entity is in a position to affect compliance. In the context of data management for FIs, the data controller makes decisions on how and why the data is processed. Whereas, the data processor only processes the data on behalf of the data controller. CSPs are typically only 'data processors' and does not make decisions or have control over how or why data is being processed, and in fact, rarely have access to

[3] https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf

[4] https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf

their customer's data. The FI typically is the 'data controller' because they make all decisions as to how and why data is being processed. An important aspect of this is how risk is allocated.

FI should perform due diligence to understand the services they are adopting and what their and the CSPs responsibilities are. Below is an example showing areas of consideration when defining responsibilities between an FI and CSP before entering into the outsourcing arrangement:

	IaaS	PaaS	SaaS
Content	FI Managed	FI Managed	FI Managed
Identity & Access Management	FI Managed	FI Managed	FI Managed
Application Security	FI Managed	FI Managed	CSP Managed
Deployment	FI Managed	FI Managed	CSP Managed
Privileged User Management	FI Managed	FI Managed	CSP Managed
Patching	FI Managed	To be Defined / Agreed	CSP Managed
Penetration Testing	FI Managed	To be Defined / Agreed	CSP Managed
Disaster Recovery Testing	FI Managed	To be Defined / Agreed	CSP Managed
Network Security	FI Managed	To be Defined / Agreed	CSP Managed
SIEM & Audit Logging	FI Managed	To be Defined / Agreed	CSP Managed
OS Management	To be Defined / Agreed	CSP Managed	CSP Managed
Storage	CSP Managed	CSP Managed	CSP Managed
Hardware	CSP Managed	CSP Managed	CSP Managed