Framework on Outsourcing to Cloud Service Providers

STATE BANK OF PAKISTAN

JANUARY 16, 2023

BANKING POLICY & REGULATIONS DEPARTMENT

Table of Contents

A. ABBREVIATIONS

AI	Artificial Intelligence
BCP	Business Continuity Plan
BoD	Board of Directors
BPRD	Banking Policy & Regulations Department
CM	Change Management
CNIC	Computerized National Identity Card
CO	Cloud Outsourcing
CSP	Cloud Service Provider
DB	Digital Bank
DDoS	Distributed Denial of Service
DoS	Denial of Service
DFI	Development Finance Institution
DR	Disaster Recovery
EMI	Electronic Money Institution
FI	Financial Institution
HA	High Availability
HSM	Hardware Security Module
IA	Internal Audit
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
ITSC	Information Technology Steering Committee
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MFA	Multifactor Authentication
MFB	Microfinance Bank
ML	Machine Learning
PaaS	Platform as a Service
PIN	Personal Identification Number
PSO	Payment System Operator
PSP	Payment Service Provider
PSP&OD	Payment Systems Policy & Oversight Department
RE	Regulated Entity
SaaS	Software as a Service
SBP	State Bank of Pakistan
SEM	Security Event Monitoring
SIEM	Security Information and Event Management
SIRT	Security Incident Response Team
SLA	Service Level Agreement

SOC	Security Operations Center
SOC Report	System & Organization Controls Report
ToR	Terms of Reference
UAT	User Acceptance Testing
VPN	Virtual Private Network
WAF	Web Application Firewall

B. DEFINITIONS

Availability	Ensuring timely and reliable access to and use of information.
Baseline	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Cloud services	Cloud computing services for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The essential characteristics of these services include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.
Cloud service provider	Means a service provider responsible for delivering cloud services under an outsourcing arrangement, and meeting the following requirements: a) At least five (5) years of experience in delivering cloud services with impeccable track record b) Have third party certifications / assessments related to IT service delivery, business continuity & disaster recovery, and cyber / information security c) Have at least Tier III certified data centers
Community cloud	A cloud deployment model where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Confidentiality	Preserving authorized restrictions on information access and disclosures, including means for protecting personal privacy and proprietary information.
Configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Cyber-attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks.
Cybersecurity incident	A cybersecurity event that has been determined to have an impact on organization prompting the need for response and recovery.
Cyberspace	A global domain within the information environment consisting of the interdependent network of information system infrastructures including the internet, telecommunication networks, computer systems, and embedded processors and controllers.

Designated Payment System Operators / Payment Service Providers	Refer to PSOs / PSPs, which are designated as Systemically Important Payment System, under Payment Systems Designation Framework issued vide PSD Circular No. 02 of 2017, amended from time to time.
Hybrid cloud	A cloud deployment model where the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.
Hyper jacking	An attack in which an adversary takes malicious control over the hypervisor that creates the virtual environment within a virtual machine host.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information assets	A collection of information, either tangible or intangible, that is worth protecting.
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Infrastructure as a Service	A cloud service model where the consumer is provided capability to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control to select networking components (e.g. host firewalls).
Integrity	Guarding against improper information modification or destruction, and including ensuring information non-repudiation and authenticity.
IT change management	IT change management is a process designed to understand and minimize risks while making IT changes. It is responsible for ensuring that IT changes are recorded, evaluated, planned, tested, implemented, and reviewed in a controlled manner.
Multi factor authentication	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Penetration testing	A testing methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Personally Identifiable Information	As defined under 'Framework for Risk Management in Outsourcing Arrangements by Financial Institutions' issued vide BPRD Circular No. 06 of 2017 and amended vide BPRD Circular No. 06 of 2019.
Platform as a Service	A cloud service model where the consumer is provided capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The

	consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Private cloud	A cloud deployment model where the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Privilege user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Public cloud	A cloud deployment model where the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider.
Recovery point objective	The point in time to which data must be recovered after an outage.
Regulate entities	Banks, MFBs, DFIs, DBs, EMIs, PSOs, PSPs, and designated PSOs/PSPs.
Security event monitoring	Security event monitoring provides real-time monitoring, correlation and analysis of activity in the environment, detecting and alerting on valid threats to the data and devices.
Software as a Service	A cloud service model where the consumer is provided capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
Supply chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services, and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Tokenization	Tokenization is a process of replacing actual sensitive data elements with non-sensitive data that has no correlation with the dataset.
Virtual private network	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.
Vulnerability assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

C. STATUS OF PREVIOUS REGULATORY INSTRUCTIONS

This framework shall have an overriding effect on cloud related directions prescribed under the following regulatory instructions:

1. Section 4.4 'Cloud Computing' of 'Enterprise Technology Governance & Risk Management Framework for Financial Institutions' issued vide BPRD Circular No. 05 of 2017 and amended vide BPRD Circular No. 04 of 2020 on 'Outsourcing to Cloud Service Providers (CSPs)'.
2. 'Framework for Risk Management in Outsourcing Arrangements by Financial Institutions' issued vide BPRD Circular No. 06 of 2019.

D. PURPOSE, SCOPE AND APPLICABILITY

1. This framework sets out minimum requirements for REs to outsource their material and non-material workloads to CSPs. However, certain requirements which are applicable only on the material workloads have been specifically mentioned. Further, REs are encouraged to put in place control measures over and above the specified requirements.
2. This framework shall:
   a) Apply to all REs;
   b) Cover all types of cloud service models (i.e. SaaS, PaaS and IaaS);
   c) Be applicable on all types of cloud deployment models (i.e. public, private, community, and hybrid).

E. PERMISSIBLE CLOUD OUTSOURCING ARRANGEMENTS

1. For the purpose of these regulations, **material workload** means all systems, applications, and services that are fundamental for carrying out business of an RE, and if disrupted, have the potential to significantly impact an institution's business operations, reputation or profitability.
2. REs may outsource their workloads to CSPs in the following manner:
   a) All type of workloads (i.e. material and non-material) may be outsourced to reputable onshore (i.e. domestic) CSPs;
   b) EMIs, non-designated PSOs/ PSPs may outsource their material and non-material workloads to offshore (i.e. outside Pakistan) CSPs;
   c) Banks, MFBs, DBs, DFIs and designated PSOs/PSPs may outsource their non-material workloads to offshore CSPs. However, outsourcing of their material workloads to offshore CSPs shall be subject to SBP approval whereby SBP may grant approval on case to case basis, after considering the following:
      i. Systemic implications of the CO arrangement
      ii. Institution specific risks
      iii. Legal and other strategic risks
      iv. Data processing and storage
      v. Availability and quality of services
      vi. Security and other controls
      vii. Contingency and exit planning
      viii. Resilience
      ix. Sub-contracting
      x. Assurance mechanism
      xi. Role and responsibilities

d) For approval to outsource material workloads to offshore CSPs, banks, MFBs, DBs and DFIs shall submit their request to BPRD whereas designated PSOs/PSPs shall submit it to PSP&OD;
e) While granting approval to banks, MFBs, DBs, DFIs and designated PSOs/PSPs, SBP may impose additional terms and conditions over and above the requirements of this framework;
f) For CO arrangements, REs may use any service and deployment model as per their requirements and risk appetite;
g) REs shall give preference to onshore CSPs for outsourcing their workloads;
h) REs shall not process and store their data in unfriendly or hostile jurisdictions;

3. Outsourcing of services to CSPs does not absolve the REs from their prime responsibilities including managing and running the business operations effectively, legal and regulatory compliance, and protection of customers' data.
4. SBP may instruct any RE to restrict outsourcing of their workloads to CSPs due to its systemic impact, unacceptable risks and any other concerns.
5. REs shall submit details of their CO arrangements to SBP, as and when required.
6. SBP may instruct REs to shift their cloud based workloads to SBP designated onshore community cloud as and when the same is available.

F. GOVERNANCE

The structure and processes for managing CO arrangement are vital for maximizing the benefits, and managing the associated risks. REs planning to outsource their workloads to CSPs need to consider adapting their organizational structure for effective and efficient oversight of CSPs, specifically pertaining to performance, operational effectiveness of controls and remediation. In this regard, REs shall ultimately be responsible and accountable for all of its information assets hosted on CSPs, and comply with the following requirements:

1. Develop a comprehensive policy for CO duly approved by their BoD. In this regard, the REs can also amend their existing 'Policy for Outsourcing Arrangements' to include/update CO. The policy shall encompass all services, as per requirements provided in section E above that can be outsourced to CSP, and at least include all those aspects that have been prescribed in this framework.
2. Conduct appropriate due diligence of CSPs and proactively identify any risks emanating from their CO arrangements including risks associated with sub-contracting by CSPs.
3. Update their Enterprise Risk Management framework or other relevant policies for effective oversight and management of risks emanating from the CO arrangement(s). The framework shall include sub-contracting risks, assessment of cloud service location(s) especially if outside Pakistan with specific focus on areas including but not limited to legal aspects; regulatory issues; jurisdictional concerns; availability; security and resilience of information assets and services; connectivity; political and security situation; ease of oversight; plausibility of RE, SBP and external audit staff to travel for onsite assessment/ audit or alternate assurance mechanism.
4. Delegate cloud specific governance responsibilities such as for overseeing adherence to regulatory as well as performance requirements, including cloud service SLAs, reviewing of KPIs and KRIs, incidents (including cybersecurity incidents) and other relevant matters to the ITSC. In this regard, the ToRs of ITSC shall be suitably amended to include these responsibilities.
5. Undertake all CO arrangements through legally binding SLAs, which shall at least include the areas prescribed in **Appendix – I**. These SLAs must be vetted by the legal function of the RE and be executed by the REs (except branches of foreign banks) themselves instead

of their parent company or subsidiary, with governing law preferably as law of Pakistan. However, compliance with the laws of Pakistan, along with compliance to any legal obligation as prescribed by the host country of the CSP, shall be mandatory at all times.

6. Define and agree upon the roles and responsibilities of the IT and operational departments (e.g. requirement analysis, performance testing, UAT, responsibility for data validation, etc.), before transferring information assets and services to a CSP.
7. Ensure that the CO arrangements are compliant with the relevant legal and regulatory requirements, and the IA functions of the REs shall provide independent certification to their BoDs in this regard.

G. DUE DILIGENCE OF CLOUD SERVICE PROVIDER

REs shall exercise reasonable care before entering into CO arrangements. To ensure effective management of the associated risks, REs shall conduct reasonable due diligence of the CSPs and their material sub-contracting arrangements by using defined criteria which shall include the following:

1. Evaluation of feasibility of CO arrangements including cost effectiveness, quality of service, and legal / regulatory / compliance risks.
2. Ability of CSP to meet legal and regulatory requirements of Pakistan.
3. Assessment of financial strength and resources.
4. Competence, business structure, experience, track record in delivering such services.
5. Assessment of CSPs ability to comply with necessary minimum controls including physical security / internal controls based on the intended workloads, especially with respect to confidentiality, integrity, availability and resilience.
6. Assessment of corporate governance and entity level controls.
7. Assessment of CSPs ability to provide REs the control over data residency enabling them to shift over preferred data center instance, depending upon the cloud service model, in order to host these services at such locations/countries/regions considering geopolitical risks.
8. Cybersecurity and IT capabilities including adherence to international standards and best practices.
9. Sub-contracting risk management.
10. Data security related controls.
11. Access, audit and information rights of REs, SBP and external auditors of the REs.
12. Support services.
13. Contingency, resilience and exit arrangements.
14. Up to date certification and attestation of the CSPs including but not limited to IT service delivery, business continuity & disaster recovery, cyber / information security, and data center Tier III certification.
15. Liability of claims / penalties on CSPs for:
    a) Unauthorized transactions;
    b) Service disruptions;
    c) Security breaches;
    d) Enforcement and penal actions that may be taken by regulatory and legal authorities against the REs for not complying the regulatory and legal requirements, due to faults by CSPs.
16. For material workloads:
    a) Threat & Vulnerability Assessment or equivalent independent assessments of data centers to identify the security and operational weaknesses. The scope of such assessments shall include physical and environmental security, perimeter security,

access controls, security & emergency procedures, monitoring, redundancy, natural disasters, and the political and economic climate of the country in which the data center resides. The assessment shall cover all data centers where the REs' data / systems will reside;

b) Independent assessments instead of solely relying on attestations by the CSPs, and the results shall be reviewed by REs' IA as well as Information Security (IS) function. However, the REs may consider SOC Reports (level 1, 2 & 3).

H. OVERSIGHT

The risk exposures and effectiveness of the corresponding controls may vary over the tenure of the CO arrangements. In this regard, REs shall:

1. Develop and maintain an effective oversight mechanism including but not limited to the assessment of performance against desired service levels and ongoing viability of the CSP and its services, cybersecurity practices and controls, changes in service location(s), sub-contracting, change of ownership, control environment; and timely response to emerging risks and issues.
2. On an ongoing basis, review and monitor the CSP's compliance with legal, regulatory and contractual obligations.
3. Monitor access to their cloud data/workloads, wherever possible such as through cloud activity reports.
4. Review internal control assessment / audit reports of the CSPs, in order to obtain assurance regarding the security and resilience.
5. For material workload, conduct comprehensive audit of the CSPs, either themselves or through third party assessors / pooled audits, at least once in two years. The scope of the audit shall at least include the infrastructure and related software used to deliver cloud services to the RE. However, in case where audit/onsite assessment cannot be conducted due to a valid reason(s), REs may rely on internationally recognized third party certifications and reports made available by the CSPs, after sufficient understanding and review of their scope, methodology and the ability of the assessors.

I. CONTINGENCY PLANNING

REs shall develop contingency plan for their CO workloads in order to deal with any disruption/degradation of cloud related services. The contingency plan shall take into account all possible scenarios regarding the unavailability of CSP related services due to various reasons such as technical/connectivity issues, inability of CSP to provide services due to legal actions in their respective jurisdictions, etc. In this regard, REs shall:

1. Prudently select appropriate implementation option (service and deployment model, availability zones, server/server-less, etc.) along with related communication technologies, to offer better resilience that commensurate with their workload.
2. Maximize the redundancy by design and workload distribution, and implement health and monitoring checks for ensuring HA of their cloud workloads.
3. Ensure redundant and robust connectivity arrangements through different international internet cables and include penalties for disruption and downtimes in their agreements.
4. Define clear roles and responsibilities including responsibility for signing off, updating and activating the contingency plan.
5. Periodically review and update the contingency plan, taking into account developments which may affect their feasibility. These may include increase in number of availability

zones, changes in business requirements, new viable alternate CSPs, technological changes, etc.

6. Periodically (at least once annually) test the contingency plan against various scenarios including disruption of internet / communication services, unavailability of CSP, etc. Where possible, REs may conduct collaborative testing of their contingency plan with their CSPs. Further, the REs shall ensure that the deficiencies identified during testing are recorded and corrective actions are implemented.

J. RIGHT TO AUDIT, ACCESS AND INFORMATION

REs shall ensure that CO does not hinder SBP in conducting its supervisory functions. In this regard, the REs shall comply with the following requirements:

1. Ensure that their internal & external auditors/ independent assessors and SBP have right to conduct audits and onsite assessments of the CSP and its sub-contractors, if required. Further, there should be no restriction or prohibition on access to REs' cloud related information assets and services for the RE, its auditors, independent assessors or SBP's authorized staff or such visits are otherwise not impractical.
2. Ensure that access, audit and information rights provided through the contractual arrangement include where relevant:
   a) Premises, data, devices, information, systems, and networks used for providing the cloud services or monitoring its performance. These may include CSP's (and its sub-contractors) policies, processes, and controls;
   b) Results of security testing carried out by CSP or on its behalf, on its applications, data, and systems to assess the effectiveness of the implemented cybersecurity processes and controls;
   c) Results of security testing carried out by the sub-contractors or on its behalf, on its applications, data, and systems, where applicable, to ascertain effectiveness of the cybersecurity processes and controls;
   d) Company and financial information;
   e) CSPs' external auditors, personnel, and premises.
3. In case, where audit/onsite assessment cannot be conducted for a valid reason(s), REs may rely on internationally recognized third party certifications, and reports made available by the CSP. However, reliance on these third party certifications and reports shall be supported by adequate understanding and review of the scope, the methodology applied therein and the ability of the third party and CSP to clarify matters relating to the assessment. Further, the REs shall have contractual right to request for the expansion of the scope of the certifications / assessments / audits to cover relevant controls and systems.
4. Ensure that CSPs timely provide any information requested by SBP, whenever required.
5. Follow up with the CSP to ensure that all appropriate and timely remediation actions are taken to address any audit findings.

K. EXIT PLANNING

REs shall develop an exit plan by considering the materiality and impact of their workloads outsourced to CSPs. In this regard, REs shall comply with the following requirements:

1. Ensure that the exit plan covers scenarios for stressed and non-stressed exit circumstances.

2. Ensure that the exit plan has defined trigger events, alternative solutions, transition plans, and roles and responsibilities including responsibility for signing off, updating and activating the plan.
3. Periodically review and test the exit plan, taking into account developments which may affect its feasibility.
4. Implement measures including but not limited to contractual or escrow arrangements, to ensure continuity of critical business services in case of exit.
5. Ensure complete removal of data including logs from all locations of CSP in case of exit.
6. To avoid the lock-in and dependency risks, REs shall in their CO arrangement contracts:
   a) Avoid inclusion of any lock-in clause or exclusivity arrangements;
   b) Ensure that they have right to terminate the CO agreement at least in the following circumstances:
      i. Change in ownership of the CSP
      ii. Insolvency or liquidation of the CSP
      iii. CSP goes into judicial administration
      iv. CSP is in breach of applicable laws, regulations or contractual provisions
      v. Significant and material breach of security or confidentiality
      vi. Demonstrable deterioration to perform the contracted service
   c) Ensure that the minimum termination period is documented in their CO contracts.

L. SUB-CONTRACTING

The CO arrangements expose REs to various risks relating to sub-contracting due to improper/non implementation of controls by the sub-contractors. For material sub-contracting, the REs shall comply with the following requirements:

1. Have visibility of the CSP supply chain by ensuring that the CSP maintains and provides an updated list of its sub-contractors.
2. Consider potential impact of large, complex sub-contracting by the CSPs on their operational resilience, and ability to oversee and monitor the emanating risks.
3. Only permit sub-contracting by CSPs if such arrangements do not give rise to excessive operational risks, and sub-contractor agrees to comply with all applicable legal, regulatory, contractual, audit and access requirements including granting REs and SBP contractual access, audit and information rights.
4. Review material sub-contracting agreements of the CSP and ascertain that the legal, regulatory, operational, and cybersecurity requirements are complied with, throughout the supply chain.
5. Ensure that the CSPs have the capability and capacity to oversee any material sub-contracting on an ongoing basis.

M. USER ACCESS MANAGEMENT AND AUTHENTICATION

REs shall implement complete life cycle of user access management for their cloud related workloads, while complying with the following requirements:

1. Implement at-least four eye principle for user access administration.
2. Periodically review user access right changes independently.
3. Ensure that the use and access of service, generic and administrative accounts are controlled and monitored. Moreover, the REs shall implement MFA and limit use of these accounts through dedicated machines only.

4. Create separate account of administrative users for routine operations, and implement enhanced password controls (length, complexity, age).
5. Implement MFA and IP source restrictions (wherever possible) for their users accessing cloud environment.
6. Monitor and document the use of master account, and permit its usage only under exceptional circumstances.
7. Implement access controls for data backups including log data, of cloud related workloads.
8. Ensure that CSPs do not have access to REs' systems, software and data.

N. CHANGE AND CONFIGURATION MANAGEMENT

REs shall plan and implement configuration management in conjunction with IT change management to ensure safe and secure operations of cloud services. In this regard, REs shall comply with the following requirements for their cloud related workloads:

1. Implement mechanism for detecting unauthorized changes to cloud environment, and configure automated alerts for the changes.
2. Ensure CM procedures for cloud related workloads are documented and mutually agreed with the CSP. These shall at least include change request and approval procedures, change prioritization and impact assessment, change reporting, roles and responsibilities, timeframe for patching and software releases.
3. Ensure that the CSPs have well-defined and robust CM controls, and notify the REs in advance of the changes.
4. Ensure that the changes are tested before their implementation on the production environment.
5. Define roles and responsibilities of REs staff for configuration management of the cloud environment, and at least segregate infrastructure, security and application roles.
6. Create and maintain baselines for cloud hosted systems, and periodically review, monitor, report and remediate non-compliance with the baselines.

O. INCIDENT MANAGEMENT

Effective and efficient remediation of the incidents requires timely detection and proper integration with the incident response and management processes. With the increase in sophistication of cyber-attacks, there is a need to use advance analytics to correlate events across multiple systems. For incident management, REs shall comply with the following requirements for their cloud related workloads:

1. Define and document criteria, performance requirements and procedures for escalation, notification, containment and closure of incidents (including IT, cyber incidents) in consensus with the CSP(s).
2. Ensure access to incident and root cause analysis reports of the CSPs.
3. Designate a SIRT to provide timely response to IT/cyber incidents. In this regard, roles and responsibilities of CSP and REs' teams shall be formalized.
4. Ensure that CSPs shall provide reasonable access to necessary information to assist in any REs' investigation arising due to an incident in the cloud.
5. Ensure that the CSPs conduct formal post incident review of the material cloud related incidents and provide their report to the RE.
6. Ensure that ITSC as part of their oversight reviews and discusses cloud related incidents.

7. Periodically review and test Incident Response Plan of cloud related workloads at least once annually, keeping in view cybersecurity as one of key considerations.

P. DATA SECURITY

Outsourcing of the workloads to the CSPs does not relieve the REs from the responsibility of safeguarding data confidentiality and integrity. In this regard, REs shall:

1. Encrypt data at rest (including backups) and in transit using strong and non-obsolete cryptographic algorithms.
2. Desensitize the production data before porting or using it on non-production environment(s).
3. Ensure that their data in the cloud environment is clearly identifiable and segregated.
4. Take appropriate measures for the protection of Personally Identifiable Information (PII); and ensure compliance with the requirements of laws of Pakistan at all times. Further, REs shall ensure that CSPs do not disclose their data to any third party including foreign governments / courts / law enforcement agencies without their consent.
5. Ensure that CSP does not use their data for any commercial purposes.
6. Implement reasonable backup and restoration testing mechanism, depending on the nature of the workloads in compliance with the defined RPOs. Further, the backup mechanism shall have ransomware protection, and the backup restoration testing exercise shall be conducted at least on a half-yearly basis.
7. Classify information assets in terms of their sensitivity, confidentiality & availability, and implement additional controls for high value cloud information assets.
8. Implement controls to prevent unauthorized exfiltration of data from the cloud environment. These controls shall include deployment of content inspection technologies, controls on data downloading and extraction, monitoring unusual data access, etc.
9. Ensure that they are notified about any proposed change in the location of their data, and have contractual right to reject such change, or terminate the CO arrangement on such grounds.
10. Ensure that data is deleted from all storage locations of the CSP following an exit or termination of the CO arrangement, and where applicable, from the systems of any sub-contractor by requesting written confirmation from the CSP.

Q. CRYPTOGRAPHIC KEY MANAGEMENT

CSPs use cryptographic controls to secure access and segregate customers' data. Hence, the security of the cryptographic keys is critical for ensuring the data security. CSPs offer a variety of key management options/features, which can be selected by the REs for implementation based on the significance of their workloads. In this regard, the REs shall comply with the following requirements:

1. Develop and implement policies and procedures governing the lifecycle of the cryptographic material.
2. Ensure that details of the cryptographic algorithms and other related parameters such as key lengths, renewals etc. are reviewed by a subject matter expert.
3. Ensure that details of the location, ownership and management of the encryption keys and HSM are agreed with the CSP and documented.
4. Ensure that the cryptographic keys are unique and generated only by the REs. Further, REs must have the sole ability to administer/manage these keys and HSM.
5. Periodically change the cryptographic keys in accordance with the international standards and best practices.

6. Ensure that the encryption keys are stored separate from the virtual images and information assets.
7. For material workloads, deploy/implement HSM with due controls.

R. TOKENIZATION

Depending on the sensitivity of data workload, REs may implement tokenization to minimize the data footprint. While implementing tokenization, REs shall assess and evaluate the features and data interactions of the tokenization solution. REs shall also ensure that the CSPs do not have access or control over the tokenization solution.

S. NETWORK ARCHITECTURE

The network structure and logical layout is of paramount importance in any cloud implementation. Therefore, the REs must implement controls for protection against plausible threats/attacks including cloud specific attacks, by implementing the following requirements:

1. Ensure security of their CO arrangements and on premise environments by implementing controls at appropriate locations to detect and mitigate security breaches and ongoing attacks. These controls shall include but not limited to perimeter security, network IDS/IPS, WAF, DDoS protection, etc.
2. Implement network segmentation based on type of workloads (e.g. production, pre-production, quality assurance, development, etc.) and purpose (e.g. end-users, critical servers, other servers, middleware, interface, etc.). In this regard, a dedicated network segment (i.e. management network) not accessible from other operational segments shall be implemented for administration purposes. Further, all internet traffic shall be routed through a dedicated network segment (i.e. security segment) and other network segments shall not have direct internet access.
3. Secure traffic between the cloud and on premise environment using a VPN or direct network connection with stringent access control rules configured to ensure routing of traffic from/to dedicated source and destination IPs.
4. Monitor and control access to and security of the cloud environments. In this regard, regularly review the firewall rules and access lists, especially after any changes.

T. SECURITY TESTING

The dynamic and evolving nature of cyber threats requires a high degree of validation and testing of security posture of an enterprise, on periodic basis. However, security testing of the systems and applications in the cloud environment is challenging due to the inherent shared service model. In this regard, REs shall comply with the following requirements:

1. Conduct vulnerability assessment, penetration testing and scenario based security testing of their systems hosted with the CSPs on periodic basis, at least once annually.
2. Ensure that CSPs conduct vulnerability assessment and penetration testing for the infrastructure and applications managed by them, at least once annually in order to provide security assurance to the REs. Further, the REs shall be fully cognizant of the scope of such assessments while examining the results.
3. Ensure that security testing is conducted while taking into consideration various scenarios and threats that are unique to cloud services including but not limited to hypervisor jumping, weak application programming interfaces, DoS hyper jacking, wrapping attacks, cloud malware injection, side channel attacks, etc.

4. Ensure that all vulnerabilities identified for their cloud related workloads are categorized in terms of risk, tracked and rectified (including post validated). For the infrastructure and applications managed by the CSPs, REs shall implement alternate mechanism for obtaining assurance that the vulnerabilities are timely rectified.
5. In case of material CO, ensure independent Threat & Vulnerability Assessment of CSP's data centers hosting the data/systems of REs, at least once annually.

U. SECURITY EVENT MONITORING

REs shall establish mechanisms for SEM by complying with the following requirements:

1. Wherever possible, leverage the controls/tools available in the cloud environment to enforce consistent security standards and baselines, automated response, remediation and notification.
2. Integrate CSP related services with their SIEM solutions to provide a detailed analysis of the security logs. In this regard, cloud specific incident scenarios with correlation rules shall be implemented. Further, AI and ML driven technologies may be explored and preferably adopted, where available.
3. Ensure that cloud related activities are effectively monitored by their SOC on 24x7 basis.

V. OTHER REQUIREMENTS

1. REs shall monitor and review capacity utilization of their cloud workloads.
2. REs shall provide adequate training of the cloud environment, to their end-users and privileged users.
3. All security incidents / breaches shall be reported to SBP in compliance with the requirements specified in the 'Enterprise Technology Governance & Risk Management Framework for Financial Institutions' or as advised by SBP from time to time. Further, REs shall conduct investigations to identify the root cause, take appropriate actions to prevent recurrence of such incidents in future and fix responsibility for such lapse.
4. For material workloads, REs shall provide following information to SBP[1] one month before placing their services with the CSPs:
   a) Name of the CSPs, and their parent company (if any);
   b) Description of the activities and details of data to be placed with the CSP;
   c) Date of commencement / renewal / expiry of services;
   d) Last contract renewal date (where applicable);
   e) Service and Deployment Models.

******

[1] Banks, MFBs, DBs and DFIs shall provide the required information to BPRD, whereas designated PSOs/ PSPs shall provide the same to PSP&OD.

Appendix – I

Areas to be included in SLAs with CSPs

1. Clear description of the outsourced activity including type of support services to be provided (containing activities / processes, service and deployment models, services offered, etc.).
2. Roles and responsibilities of contracting parties including responsibilities at the time of recovery and resolution.
3. Ownership and access of assets.
4. Term of contract along with renewal and notice periods.
5. Governing law of the agreement.
6. Financial obligations of the parties.
7. Permitted and restricted activities for sub-contracting.
8. Requirement that CSPs shall be solely responsible for the sub-contracting including oversight of their sub-contractors.
9. Requirement of obtaining prior written authorization from the RE before transferring information assets and services/ servers.
10. Mechanism for data portability and purging in case of exit.
11. Prohibition of access of REs' systems, software and data to CSP and its sub-contractors.
12. Prohibition on sharing data of RE with any other entity including any host country regulatory or law enforcement authorities without taking REs' prior written approval.
13. Advance notification of change in material sub-contractors of CSPs.
14. Right of the REs to approve or deny material sub-contracting by CSPs or related significant changes. Further, REs shall have right to terminate the contract if these changes give rise to unacceptable risks.
15. Location(s), where the service will be provided, data kept-processed-stored. Requirement for the CSP to provide reasonable notice to the RE if it proposes to change the said location(s). Contractual right to reject any proposed change to the location of data, or terminate the cloud outsourcing arrangement on such grounds.
16. Data accessibility, availability, integrity, confidentiality and security related provisions.
17. Service levels including qualitative and quantitative performance criteria, and right of RE to monitor CSPs' performance on an ongoing basis (reference to KPIs and KRIs shall be made in the SLA).
18. Reporting obligations of the CSP to the RE, including to notify of any development that can have material impact on the CSPs' ability to deliver the agreed service levels.
19. Mandatory insurance coverage (if any) against certain risks.
20. Development and testing of contingency plans for both parties including BCPs.
21. Provisions to ensure that the data owned by the RE can be accessed promptly in the case of insolvency, resolution or discontinuation of business operations of the CSP.
22. Access, audit and information rights of the REs and SBP including right to inspect and audit, access or seek information, from the CSP and its sub-contractors with regard to the outsourced services for assurance, oversight, incident investigation, inspection or any other purpose. In case of offshore CSP, REs may rely on internationally recognized third party certification and reports made available by the CSP; however, the RE shall include contractual right in their SLAs to request for scope expansion of the certifications / assessments / audits to cover relevant controls and systems.

23. Assessment, certification and audit reports to be provided by the CSP to REs, generally on periodic basis and specifically on demand e.g. System and Organization Controls (SOC) level 2 and level 3 reports, on annual basis.
24. Cybersecurity related expectations including data security, network security, security testing and monitoring, etc.
25. CM procedures including terms, notification and testing requirements, etc.
26. Threat and Vulnerability Management related requirements including vulnerability rectification timeframe based on the risk category, post validation, notification & communication, related procedures, etc.
27. Operational and security incident handling procedures including escalation and reporting.
28. Termination rights and exit strategies covering both stressed and non-stressed scenarios.
29. The agreement must not contain any lock-in clause.
30. In case of exit, REs shall have contractual rights to continue with the arrangement until such time, it is able to switch to a substitute arrangement.
31. Payment and pricing.
32. Contractual remedies including enforceable liquidity damage clauses, etc.
33. Dispute Resolution provisions.

******