पेंशन निधि विनियामक एवं विकास प्राधिकरण
PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

Azadi Ka Amrit Mahotsav

CIRCULAR

Circular no: PFRDA/2023/33/ICS/01 **23rd November 2023**

To

All Intermediaries registered with PFRDA

Subject: Adoption of cloud services by intermediaries regulated by PFRDA

This circular is issued in exercise of powers conferred under Sec 14(1) read with sec 14(2) clause (a) of the PFRDA Act, 2013 and to protect the interests of subscribers. The circular is being issued to enable and equip the intermediaries with a policy framework on adoption of cloud services by intermediaries for the services being rendered by them. The policy also lays down the regulatory and legal requirements and compliances by the intermediaries, if they adopt the cloud services.

1. Intermediaries registered with PFRDA have been extensively leveraging Information Technology (IT) and IT enabled services (ITeS) including adopting cloud services to support their business models and products and services offered to their customers.
2. Adoption of cloud services for delivering the IT services is increasing in financial services sector and is also being encouraged by the government through various initiatives. While cloud solutions offer multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., it also increases cyber security risks and challenges.
3. PFRDA has earlier issued guidelines on outsourcing of activities for Central Recordkeeping Agencies vide its circular no **PFRDA/2016/4/CRA/TB/2 dt.29/01/2016** And for pension funds vide its circular no: **PFRDA/2017/30/PF/4 dt.09/10/2017** which were basically meant for policy on day to day handling of the operations and do not cover the outsourcing activities pertaining to IT and ITeS.
4. In view of the above, the Authority puts in place a framework or policy on adoption of cloud services by registered intermediaries to address the risks effectively and ensure regulatory compliance. The said policy shall be in addition to the referred outsourcing guidelines and the adoption of cloud services shall be considered as part of the outsourcing of the activities by the registered intermediaries.
5. The intermediaries who have already adopted or those intend to adopt cloud services are hereby advised to comply with the policy which is being attached as **Annexure.**

The circular is issued with the approval of the Competent Authority.

K.R.Daulath Ali Khan,
General Manager
Information and Cybersecurity Dept

बी–14/ए, छत्रपति शिवाजी भवन, कुतुब संस्थागत क्षेत्र, कटवारिया सराय, नई दिल्ली–110016
दूरभाष : 011–26517501, 26517503, 26133730, फैक्स : 011–26517507, वेबसाईट : www.pfrda.org.in
B-14/A, Chhatrapati Shivaji Bhawan, Qutub Institutional Area, Katwaria Sarai, New Delhi-110016
Phone : 011-26517501, 26517503, 26133730, Fax : 011-26517507, Website : www.pfrda.org.in

आज़ादी का अमृत महोत्सव

ANNEXURE

POLICY ON ADOPTION OF CLOUD SERVICES BY INTERMEDIARIES REGULATED BY PFRDA

Background:
Intermediaries registered with PFRDA have been extensively leveraging Information Technology (IT) and IT enabled services (ITeS) including adopting cloud services to support their business models and products and services offered to their customers. Further, there have been several requests by the intermediaries to PFRDA for allowing them to adopt cloud services for storage of data and related applications associated with NPS, APY and other pension schemes.

In the recent times the adoption of cloud services for delivering the IT services is increasing and is also encouraged by the government through various initiatives. While cloud solutions offer multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., entities adopting such technology should also be aware of the new cyber security risks and challenges which cloud solutions introduce.

PFRDA has earlier issued guidelines on outsourcing of activities for Central Recordkeeping Agencies vide its circular no **PFRDA/2016/4/CRA/TB/2 dt.29/01/2016** And for pension funds vide its circular no: **PFRDA/2017/30/PF/4 dt.09/10/2017**. These were basically meant for policy on day-to-day handling of the operations and do not cover the outsourcing activities pertaining to IT and ITeS in detail. Further, the registration guidelines issued by the Authority for intermediaries like CRAs, PFs etc., also provide for adoption of emerging technologies like cloud computing.

In view of the above, the Authority after reviewing the existing arrangements has decided to come out with a framework or policy on adoption of cloud services by registered intermediaries to address the risks effectively and ensure regulatory compliance. The said policy shall in addition to the referred outsourcing guidelines and the adoption of cloud services shall be considered as part of the outsourcing of the activities by the registered intermediaries.

1. Applicability
The provisions of this policy shall be applicable to all the registered intermediaries of PFRDA.

2. Definitions: for the purpose of this policy, unless the context otherwise requires;

i. BCP means Business Continuity Plan
ii. CISO means Chief Information Security Officer
iii. Cloud services means infrastructure, platforms, or software that are hosted by third party providers and made available to users through the

internet and includes cloud computing.

iv. Cloud computing means Cloud computing is a model 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- (as defined by NIST (National Institute of Standards and Technology - US)).

v. CSP means Cloud Service Provider

vi. Intermediary includes pension fund, central recordkeeping agency, National Pension System Trust and point of presence in terms of PFRDA Act, 2013.

vii. SOC means Security Operation Center

3. Purpose:

The underlying principle of the policy is to lay a framework for adoption of technological advances so that the intermediary ensures that adoption of technological advances like adoption of cloud services neither diminish its ability to fulfil its obligations to subscribers nor impede effective supervision by the authority with due assessment of the attendant risks. Intermediary while adopting cloud services or other IT enabled services shall take steps to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by the intermediary if the same activity was not outsourced.

4. Cloud Services

There are several popular cloud deployment and service models that have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity. Each of these models come with corresponding service, business benefit and risk profiles. The intermediaries shall examine the following while adopting clud services for discharge of their functions:

a. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.

b. In engaging cloud services, intermediaries shall ensure, inter alia, that such outsourcing addresses the entire lifecycle of data, that is, covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The intermediary shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.

c. In adoption of cloud services, intermediaries shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attended risks while establishing appropriate risk management framework.

d. Cloud Governance: intermediaries shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, inter alia, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.

5. Policy and principles for adoption of cloud services by intermediaries

The following shall be the broad policy and principles to be followed and adhered by all registered intermediaries of the Authority for adoption of cloud services:

a. The Board of the intermediary shall decide upon the matter of adoption of Cloud based services after due evaluation of the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing.

b. The Board of the intermediary shall consider all relevant laws, regulations, rules, guidelines and conditions of approval licencing or registration, when performing its due diligence in relation to adoption of cloud services. The due diligence referred shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. The Intermediary shall be responsible and accountable for all aspects related to such outsourcing of functions including the cloud services. Such accountability shall encompass availability of cloud applications, confidentiality, integrity and security of its data and logs, and ensuring Intermediary's compliance with respect to the Act, rules, regulations, circulars, etc. issued by PFRDA, if the intermediary decides to adopt cloud services.

c. The Board after due evaluation of all relevant activities, shall put in place a comprehensive Board approved cloud adoption policy including laying clear policy on the role of Senior Management, IT function including the role of CISO, business function, and oversight & assurance functions in respect of adoption of cloud services. It shall further cover the criteria of selection of service providers, delegation of authority depending on risk and materiality for various activities related to such adoption, data localization, data ownership, access, risk assessment and due-diligence on cloud service providers(CSPs), security controls, disaster recovery and business continuity plans, systems to monitor and review the operations of these activities and termination processes and exit strategies, vendor lock-in, including business continuity in the event of a third-party service provider or CSP exiting the arrangement.

d. Such board approved policy shall also contain details of audit and assurance activities in relation to such adoption of cloud services. The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, inter alia, aspects such as roles and responsibilities of both intermediary and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response and resilience preparedness and testing, etc.

e. The storage/ processing of data (DC, DR, near DR etc.) including logs and any other data pertaining to the intermediary in any form in cloud should reside/be processed within the legal boundaries of India. Data collection and processing of data must be governed by the laws and policies of India and shall be in compliance to the various regulations, guidelines issued by Ministries / Departments and Government agencies from time to time. Further, the data should reside/ be processed within the MeitY empanelled Cloud Service Providers' data centres holding valid STQC (or any other equivalent agency appointed by Government of India) audit status.

f. The Intermediary shall retain the complete ownership of its data and associated data, encryption keys, logs etc. residing in cloud.

g. There shall be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the cloud services between the intermediary and CSP. Ideally, there shall be no "shared responsibility" or "joint ownership" for any function/ task/ activity between the intermediary and CSP. If any function/ task/ activity has to be performed jointly by the intermediary and CSP, there shall be a clear delineation and fixing of responsibility for each sub-task/ line-item within the task. The aforementioned delineation of responsibilities shall be added explicitly in the agreement signed between the intermediary and the CSP. For example, the security of' the data residing in the Cloud will be the responsibility of the end user and the security of the Cloud Infrastructure level will be the responsibility of the Cloud Service Provider (CSPs).

h. Intermediaries shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. Intermediaries shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the Intermediary. Multi-tenancy environments should be protected against data integrity and confidentiality risks and against co-mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the cloud architecture should not result in data/ information security compromise.

i. Cloud Services Management and Security Considerations: The intermediary shall take into account the subject matters as detailed in **Annexure I** regarding the cloud services management and security and ensure that the same are complied with.

j. The intermediary shall finalise the setup, architecture of the systems and cloud architecture keeping in view of the Cyber security, scalability, integrity and resilience of the systems and PFRDA shall not be liable in any manner or responsible for the functional or operational efficiency or technical aspects of such configurations.

k. Intermediaries shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements cast under Indian laws and the rights

available thereunder to Intermediaries, including those relating to aspects such as data storage, data protection and confidentiality.

l. Intermediaries shall ensure that their rights and obligations and those of the cloud service providers (CSPs) are clearly defined and set out in a legally binding written agreement. In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the intermediary, the associated risks and the strategies for mitigating or managing them. The agreement shall be sufficiently flexible to allow the intermediary to retain adequate control over all the activities in relation to the cloud services and the right to intervene with appropriate measures to meet legal and regulatory obligations.

m. The intermediary shall have incident management policy, procedures and processes in place. The intermediary shall adhere with the same for deployments being done in cloud.

n. The above referred agreement inter alia at minimum shall ensure that the following aspects are covered:

   i. compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer data;
   ii. details like scope of services, charges for services and maintaining confidentiality of customer's data, Availability of Cloud services, Performance, Security, Disaster recovery and data backup management, etc.
   iii. the deliverables, including Service-Level Agreements (SLAs) formalising performance criteria to measure the quality and quantity of service levels and other relevant issues; the exit strategy and service level stipulations in the SLA shall factor in, inter alia,

      1. contract duration;
      2. agreed processes and turnaround times for returning the intermediary's service collaterals and data held by the CSP;
      3. data completeness and portability;
      4. secure purge of intermediary's information from the CSP's environment;
      5. smooth transition of services; and
      6. unambiguous definition of liabilities, damages, penalties and indemnities.
      7. should specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the intermediary's business, while maintaining integrity and security. While migrating from one CSP to another. various clauses such as data transfer charges, deletion of data guidelines should be explicitly mentioned in contract document.

   iv. storage of data only in India;
   v. clauses requiring the service provider to provide details of data (related to intermediary and its customers) captured, processed and stored, data retention/archival;

vi. controls for maintaining confidentiality of data of intermediaries and its customers', and incorporating service provider's liability to intermediary in the event of security breach and leakage of such information;
vii. specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;
viii. contingency plan(s) to ensure business continuity and testing requirements;
ix. right to conduct audit of the CSP by the intermediary (limited to its usage of CSP services), whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the intermediary;
x. right to seek information from the CSP about the third parties (in the supply chain) engaged by the former;
xi. recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow PFRDA or person(s) authorised by it to access the intermediary's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the CSP in relation to the cloud services;
xii. including clauses making the cloud service provider contractually liable for the performance and risk management practices of its sub-contractors, if any;
xiii. termination rights of the intermediary, including the ability to orderly transfer the proposed cloud services arrangement to another service provider, if necessary or desirable.
xiv. obligation of the cloud service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the intermediary;
xv. that incidents, including cyber incidents and those resulting in disruption of service and data loss/ leakage are reported to them by the cloud service provider immediately but not later than one hour of detection to the intermediary.

o. Intermediaries shall ensure availability of qualified human resource personnel for cloud administration, monitoring and surveillance.

p. The intermediaries shall immediately notify the Authority (PFRDA) in the event of breach of security and leakage of confidential customer related information. The compliance officer of the intermediary shall be responsible for filing the incident or event reporting to CERT-In or such similar entities and including PFRDA. Information and Cyber Security breaches may be informed as per prescribed TAT to CERT-In as per PFRDA Circular dated 30th June 2021.

q. The policy/principles stated above shall also be applicable to all those intermediaries who have already adopted cloud services upon approval by PFRDA and also to those who propose to adopt such services. For those who have already adopted the cloud services for their operations, such an intermediary shall file a compliance report on the adherence to these guidelines within 120 days of issuance of this circular and PFRDA reserves the right to extend this timeline only in exceptional circumstances.

r. The intermediaries interested in adoption of cloud services shall seek approval from the regulations department of the authority to whom they report and through the compliance officer inter alia confirming that they are going to adhere to the directions/policy/advisories mentioned in the policy, providing the complete details of proposed adoption of cloud services, strategy being adopted and the framework being put in place for such adoption. Once, the cloud services adopted are in place, complete documentation with respect to the said adoption shall be provided to the Authority. The supervisory division/department may issue the guidelines including the formats of reporting to the Authority on the said cloud adoption and management in due course.

s. The policy shall be reviewed at least once in two years, any changes proposed shall be approved by the Chairman and the same shall be put up to the Board for information.

ANNEXURE I

Cloud Services Management and Security Considerations:

1. **Service and Technology Architecture:** Intermediaries shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. Intermediaries shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the Intermediary. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks and against co- mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the cloud architecture should not result in data/ information security compromise.

2. **Identity and Access Management (IAM):** IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges' and require the intermediary's approval and monitoring. In addition, multi-factor authentication should be implemented for access to cloud applications.

3. **Security Controls:** Intermediaries shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the Intermediary; necessary procedures to authorise changes to cloud applications and related resources. The Intermediaries shall ensure that the CSPs shall comply to latest version of Cloud Security ISO Standards like ISO 27017, ISO 27018 and shall ensure at least 128-bit encryption is used by CSPs to encrypt and decrypt data or files.

4. Robust Monitoring and Surveillance: Intermediaries shall accurately define minimum monitoring requirements in the cloud environment.

5. Retention of relevant logs in cloud shall be ensured for real-time incident reporting and handling of incidents relating to services deployed on the cloud. Appropriate integration of logs, events from the CSP into the intermediary's SOC, wherever applicable.

6. The intermediaries' own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / intermediary

shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.

7. Any interface which is exposed to public at large in internet in the form of a service/API/etc. is considered as internet facing interface. Adequate security controls such as IPS, Firewall, WAF, Anti DDOS, API gateways etc. should be in place and additional controls such as 2FA authentication, SSL VPN solutions should be considered. Similarly, Interfaces connected between intermediary's/relevant organizations (Through P2P or LAN/MPLS etc.) and CSP, Security controls such as IPS, Firewall, WAF, Anti DDOS, etc. shall be in place and additional controls such as IPSEC VPN wherever necessary shall be adopted. Intermediaries are required to ensure IPv6 compliance when procuring network security resources, configurations and other linked items.

8. Intermediary shall adopt appropriate Secure Software Development Life Cycle (SSDLC) processes, and security shall be an integral part right from the design phase itself.

9. To ensure the confidentiality, privacy and integrity of the data, best practices as per prevailing technological trends and procedures of encryption shall be adopted by the intermediary.

10. **Vulnerability Management:** Intermediary's shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities. The intermediary shall have a well-defined Vulnerability Management policy in place and should strictly adhere with the same. The policy should also address the vulnerability management aspects of the infrastructure /services/etc. managed by intermediary in the cloud. The cloud infrastructure shall be up to date in terms of patches/OS/version etc. The patch management policy shall cover the infrastructure of cloud and the policy shall mandate timely patch application.

11. **Vulnerability Assessment and Penetration Testing (VAPT):** The VAPT activity undertaken by intermediary should also cover the infrastructure and applications/services hosted on cloud solution. The VAPT Tactics, Tools and Procedures should be fine-tuned to test and assess the cloud native risks and vulnerabilities. VAPT should also be conducted before commissioning of any new system.

12. The intermediary's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the intermediary can continue its critical operations with minimal disruption of services while ensuring integrity and security.

13. In-house Security Operations Centre (SOC) solution of intermediary shall be integrated with the infrastructure of cloud. Outsourcing of SOC operations has the risk of data being stored and processed at an external location and managed by a third party (Managed Security Service Provider (MSSP)) to which intermediaries have lesser visibility. To mitigate the risks, in addition to the controls prescribed, intermediaries shall adopt the below mentioned

requirements in the case of outsourcing of SOC operations:

a) unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);

b) ensure that the intermediary has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the intermediary);

c) assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;

d) integrate the outsourced SOC reporting and escalation process with the intermediary's incident response process; and

e) review the process of handling of the alerts / events.

14. Backup and recovery solution

a) The intermediary shall ensure that a backup and recovery policy is in place to address the backup requirement of cloud deployments. The backup and recovery processes shall be checked at least twice in a year to ensure the adequacy of the backups.

b) The backup shall be logically segregated from production/dev environment to ensure that the malware infection in production systems should not percolate to backup environment.

c) When CSP's backup services are utilized, adequate care should be taken with encryption solution and key management.

****