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

वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

Circular No: PFRDA/2024/04/Sup-CRA/01 **Date: 21st February 2024**

To / प्रति

The CEOs of the registered CRAs/ पंजीकृत सीआरए के सीईओ

Subject: Risk Management Framework for the Central Recordkeeping Agencies (CRAs) under NPS architecture

This circular is issued in exercise of powers conferred under Sec 14(1) read with Sec 14(2) clause (e) of the Pension Fund Regulatory and Development Authority Act, 2013 and Regulation 26(2)(c) of PFRDA (Central Recordkeeping Agency) Regulations, 2015.

2. In order to ensure that the CRAs render, at all times, high standards of service, exercise due diligence, ensure proper care in their operations and protect the interests of subscribers in terms of Section 14 (2) (e) of the PFRDA Act, 2013, PFRDA hereby lays down, the following Risk Management Framework as per **Annexure I** for the guidance of the CRAs and to be designed, developed and implemented by them.

3. The risk management framework emphasizes on the importance of internal control systems, procedures and safeguards to be built into the CRA systems for safeguarding the interests of the subscribers.

4. The risk management framework to be developed by the CRAs as envisaged under this circular shall be submitted to the

विषय: एनपीएस स्थापत्य के अंतर्गत केंद्रीय अभिलेखपाल अभिकरणों (सीआरए) हेतु जोखिम प्रबंधन ढांचा

यह परिपत्र, पेंशन निधि विनियामक और विकास प्राधिकरण अधिनियम, 2013 की धारा 14(1) के साथ पठित धारा 14(2) खंड (ङ) और पीएफआरडीए (केंद्रीय अभिलेखपाल अभिकरण) विनियम, 2015 के विनियम 26(2)(ग) के अंतर्गत प्रदत्त शक्तियों का प्रयोग करते हुए जारी किया गया है।

2. यह सुनिश्चित करने के लिए कि, पीएफआरडीए अधिनियम, 2013 की धारा 14(2)(ङ) के अनुरूप, सीआरए द्वारा सेवा के उच्च मानक सदैव प्रदान किए जाएं, उचित परिश्रम किया जाए, उनके संचालनों में उचित सावधानी बरती जाए और अभिदाताओं के हितों का संरक्षण किया जाए, पीएफआरडीए एतद्द्वारा सीआरए के मार्गदर्शन के लिए **अनुलग्नक I** के अनुसार निम्नानुसार जोखिम प्रबंधन ढांचा निर्धारित करता है, जिसे सीआरए द्वारा संरचित, विकसित और कार्यान्वित किया जाना है।

3. यह जोखिम प्रबंधन ढांचा, अभिदाताओं के हितों के संरक्षण के लिए सीआरए प्रणालियों में निर्मित किए जाने वाले आंतरिक नियंत्रण प्रणालियों, प्रक्रियाओं और सुरक्षा उपायों के महत्त्व पर बल देता है।

4. सीआरए द्वारा विकसित किया जाने वाला जोखिम प्रबंधन ढांचा, जो इस परिपत्र के अंतर्गत

Authority within 120 days from the date of the issuance of this circular. Any exception to the timelines stipulated shall be supported with cogent reasons and with prior approval of the Authority.

5. This circular is issued with the approval of the Competent Authority.

परिकल्पित है, को इस परिपत्र के जारी होने की तिथि से 120 दिनों के भीतर प्राधिकरण में प्रस्तुत करना होगा। इस निर्धारित समय-सीमा में किसी भी अपवाद को ठोस कारणों और प्राधिकरण के पूर्व अनुमोदन के साथ रखा जाएगा।

5. यह परिपत्र सक्षम प्राधिकारी के अनुमोदन से जारी किया गया है।

Digitally signed by
K MOHAN GANDHI

(K Mohan Gandhi)
Chief General Manager

Annexure- I/अनुलग्नक I

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

RISK MANAGEMENT FRAMEWORK FOR CENTRAL RECORDKEEPING AGENCIES (CRAs)

Ver 1 dt 21st Feb 2024

Table of Contents

RISK MANAGEMENT FRAMEWORK FOR CRAs

Definitions

For the purposes of this risk management framework, the following definitions shall apply:

1. ‘Cyber risk’ includes any reasonably identifiable circumstance in relation to the use of network and information systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialised, may compromise the security of the network and information systems, of any technology-dependant tool or process, of the operation and process’ running, or of the provision of services, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects;
2. ‘Cyber incident’ includes an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, stores or transmits, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the CRA;
3. ‘Cyber-attack’ means a malicious cyber incident by means of an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset perpetrated by any threat actor;
4. ‘Information and communication technology (ICT)’ risk means the current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which may compromise the availability, integrity, accessibility and security of such infrastructures and of data.
5. ‘Vulnerability’ means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a threat;

A. Framework and Applicability

1. The Risk Management Framework shall be applicable to all registered Central Recordkeeping Agencies (CRAs) registered with the Authority.
2. Risk Management Framework for CRAs is an approach to managing risks associated with the operations of CRAs in a measured and a fair measure of reasonableness. The purpose of the framework is to ensure that the operations do not result in any deficiencies in service to customers, prevention of fraud, disruption, or any issues effecting the integrity of recordkeeping, accounting, administration functions of the CRAs, to the extent possible.
3. As part of the overall risk management framework, a CRA shall adopt best governance practices for risk management in the discharge of its functions and shall constitute a Risk Management Committee for better management of risks emanating from the operations being carried out. The Board of CRA shall constitute such a committee preferably with internal and external specialists who have knowledge of recordkeeping functions or IT systems or audit and accounting or any other related field. The Risk Management Committee shall draw up a Risk Management Policy and place the same before its Board for its approval.

4. CRAs may be exposed to various kinds of risk wherein the possibility of an event occurring and adversely affecting the desired objective is present. For the purpose of understanding, the associated risks can be broadly categorized as below, based on probability of occurrence and its impact and the CRAs shall adequately plan for addressing these risks:

   a. Operational Risk - The risk of losses due to inadequate or failed internal processes, people and systems or from external events. This includes Cyber risk and threat of Cyber-attacks.

   b. Fraud Risk - Intentional act committed to secure an unfair or unlawful gain and causing a financial loss to CRA, subscribers or any other stakeholder.

   c. Legal Risk - Risk of not having sufficient basis for legal recourse in the event of a dispute or litigation filed by or against the company.

In dealing with the above risks, CRAs shall be responsible for any acts of omission or commission of its employees and agents in respect of the conduct of its business including for any loss that may have been caused to subscribers by the wrongful act, negligence, fraud or default of the CRA or the vendors of CRA to whom the work has been outsourced by CRA or by an employee of the CRA. Also, CRA will be responsible for any loss or damage caused to subscribers or the stakeholder arising out of any deficiencies in design and implementation of the IT systems and which are reasonably not expected from a professional recordkeeping agency.

B. Objective of the Risk Management Framework

i. To manage associated risks through an objective assessment and in a consistent manner across the organisational set up of the CRA.

ii. A strong risk culture: managing risk shall be part of the work culture of the CRA.

iii. To put in place an appropriate risk mitigation and avoidance policy: As professional agencies, CRAs are aware of the risks they are exposed to and accordingly they shall identify the material risks and put in place an objective based risk mitigation and avoidance policy.

iv. CRAs to have sufficient controls in place to ensure that they only take the right type and amount of risk to protect the interests of the subscribers and grow their business safely and securely.

v. Deliver fair outcomes for subscribers: maintain an orderly and transparent operation of services to subscribers and all other stakeholders.

C. RISK MANAGEMENT FRAMEWORK:

The risk management framework is a guiding tool for the CRAs for designing, developing, implementation and maintenance of the CRA systems and in discharge of functions assigned to them under the PFRDA (Central Recordkeeping Agency) Regulations, 2015, and amendments thereof:

It is expected that;

i. As part of the CRA operations and management, CRAs shall formulate a comprehensive Risk Management Framework through its Risk Management Committee (RMC) encompassing the guidance provided hereunder. Such framework shall be placed before the Board of the CRA for approval and post approval of the Board, the same shall be implemented in both letter and spirit. The Board of the CRA should review the framework at least once in a financial year with an objective of strengthening and improving the risk appetite and risk management system of the CRA in all its endeavours including cyber security and resilience of operations.

ii. The RMC while drafting the said framework should also consider the relevant and appropriate principles which are laid down by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), the nodal agency under Section 70 A(1) of the Information Technology (Amendment) Act, 2008, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time. Further, the CRAs shall incorporate the material implications from the Digital Personal Data Protection Act, 2023, in the referred Risk Management Framework in order to protect and secure personal data of subscribers as is envisaged under the said Act.

iii. RMC shall also document and implement the learnings from previous instances of frauds/prevented frauds to ensure that similar incidents do not occur again.

iv. The Risk Management Framework (RMF) referred above shall provide for a set of standards and principles comprising of the following:

a. Governance and organisation

b. Operational Risk Management

c. Risk Assessment and Control

d. Fraud prevention controls

e. Supplementary Risk Mitigation Measures

f. Quality policy

g. Any other measure which aids the Risk management process.

The indicative itemised details of the above are as below:

a. Governance and organisation

The management of CRA shall define, approve, oversee and be accountable for the implementation of the risk management framework. For the purposes of corporate governance of the CRA and managing the risks in an orderly manner, the management shall:

a) Be responsible for managing the risks associated with design, development and operations of CRA systems including Information and Communication Technology (ICT) risks.

b) set clear roles, responsibilities and accountability for all activities which form integral part of the CRA functions.

c) determine the appropriate risk tolerance level of each risk identified.

d) approve, oversee and periodically review the implementation of the overall risk management policy including Cyber security policy, Business Continuity Policy and Disaster Recovery Plan.

e) approve and periodically review the audit plans associated with implementation of risk management policy approved by the Board. This shall include the usage of ICT services provided by third-party service providers;

f) be duly informed about cyber incidents, their impact, the response, recovery and corrective measures taken. The management shall examine the adequacy of risk management systems with respect to all such incidents and take appropriate measures to minimise such risks, in future.

g) identify potential risk areas including fraud, develop and put in place Red Alerts (explained later) that shall be created for identified risks and scenarios. This shall include events that may affect the business objective and lead to financial loss to the subscriber or to the CRA.

From the governance standpoint, Board level supervision shall regularly examine the working of the Risk Management Committee, an audit committee and any other committee as deemed fit for the purpose of effective design, development and implementation of risk management policy of the CRA.

The management of the CRA shall put in place adequate mechanism and controls to ensure that the integrity of the automatic data processing systems is maintained at all times and take all precautions necessary to ensure that the records are not lost, destroyed or tampered with and in the event of loss or destruction, ensure that sufficient back up of records is available at all times at a different place.

b. Operational Risk Management Policy

CRAs shall have a sound, comprehensive and well-documented operational risk management policy, which enables them to address any risk arising thereon quickly, efficiently and comprehensively. As part of the policy, CRA shall put in place detailed operation manual(s) covering all aspects of its functioning, including the interface, mode and manner of accessing CRA systems, transmission of information between the subscribers, nodal offices, POPs, PFs and all other stakeholders involved in receipt and processing of information related to NPS and other pension schemes.

The risk management policy shall have an action plan for:

a) Protecting physical components and infrastructures including computer hardware, servers, as well as all relevant premises, data centres and sensitive designated areas, including protecting the systems from cyber related risks and threats, and

b) regular upgradation of the IT systems and software, to ensure that the CRA systems are able to deliver the best of the services with latest technological advantages, adequately protected from risks including damage and unauthorized access or usage.

c) minimising the impact of various risks identified by it by deploying appropriate strategies, policies, procedures, protocols and tools as determined in the risk management policy.

d) implementing an information security management system based on recognized international standards and shall regularly review it. For this purpose, the CRAs shall have a specific "Information Security" policy.

e) segregation of management functions, control functions, and internal audit functions for a clear demarcation of responsibility and accountability.

The risk management policy referred to in paragraph 1 shall be documented and reviewed at least once a year, as well as upon the occurrence of any cyber incident.

The risk management policy referred to in paragraph 1 shall include provisions for auditing of the operations on a regular basis to ascertain the adherence to the policy by the CRA and by auditors possessing sufficient knowledge, skills and expertise in ICT and process management. Such audits shall be conducted at least once in a year and the reports thereon shall be placed before the board of the CRA after due examination by audit and risk management committees.

A formal follow-up process, including rules for the timely verification and remediation of critical audit findings, shall be established, taking into consideration the conclusions from the audit review while having due regard to the nature, scale and complexity of the CRA services and activities.

The risk management policy referred to in paragraph 1 shall include the methods to address ICT risk and attain specific objectives, by:

a) explaining how the ICT risk management framework supports the CRA's business strategy and objectives;

b) establishing the risk tolerance level for each of the identified risk, in accordance with the risk appetite of the CRA, and analysing the impact tolerance of disruptions, if any;

c) setting out clear information security objectives;

d) explaining the ICT reference architecture and any changes needed to reach specific business and compliance objectives;

e) outlining the different mechanisms put in place to detect, protect and prevent impacts of cyber incidents;

f) defining a holistic out sourced vendor strategy for ICT services at entity level showing key dependencies on third-party service providers and explaining the rationale behind the procurement of such third-party service providers in view of the risks that may emanate from such engagement;

g) outlining a communication strategy in case of cyber incidents.

The risk management policy referred to in paragraph 1 shall include obligation of CRAs for maintaining updated systems, protocols and tools in order to control or mitigate all and any potential risks and which fulfil the following conditions:

a) the systems and tools are appropriate to the nature, variety, complexity and magnitude of operations supporting the conduct of their activities;

b) they are reliable;

c) they have sufficient capacity to accurately process the data necessary for the performance of activities and the provision of services in time, and to deal with peak orders, message or transaction volumes, as needed, including in the case of introduction of new technology;

d) they are technologically resilient to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.

e) The systems have been designed to minimise the risk of fraud or being mis-used by internal or external players.

c. Risk Assessment and Control

Risk and control assessment framework is to identify critical or emerging risks proactively to take necessary risk mitigation measures, assess and manage risks impacting the business objectives of the Company/CRA. The scope of such risk assessment and control shall be as follows:

a) To assess the nature of the risk relative to the specific function

b) Evaluate the nature of the process and the underlying factors - both internal and external that could give rise to the risk event.

c) Susceptibility to fraud or theft.

d) Complexity of the of the process activities.

e) Level of judgment required to perform the process.

f) How relevant and credible data (or historical data) is available to assess the risk impact and likelihood of occurrence.

Broadly, the following steps shall be undertaken by the intermediary to arrive at proper risk assessment and controls and which form the bedrock of the risk management framework:

1. Risk assessment

- CRAs shall conduct risk assessments either by themselves or through external experts. Risk assessment so done should identify threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications.
- CRAs should identify and assess the risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
- Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected.
- CRAs shall classify the assets into critical, medium and normal risk based on the potential risk factors associated with such assets. They should identify critical assets based on their sensitivity and criticality for business operations, services, potential for fraud or cyber incidents and data management.

2. Design and implementation

CRAs should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and coordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and nontechnical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. The CRA shall plan for all efforts to 'Protect' assets by deploying suitable controls, tools and measures.

In order to protect the assets from potential risks, policies with respect to the following shall be clearly laid down and adhered to by the CRA at all times:

- Access Controls
- Physical security
- Network Security Management
- Security of Data
- Hardening of Hardware and Software
- Application Security and Testing
- Patch Management
- Disposal of systems and storage devices
- Vulnerability Assessment and Penetration Testing (VAPT)
- Upgradation of the systems –assessment and upgradation, frequency and periodic review process.

3. Security management

CRAs should adopt a comprehensive approach to security management. Security management should be based on risk assessment, be dynamic in nature, encompassing all levels of CRA's activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security.

CRAs should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.

a. Response

CRAs should act in a timely and co-ordinated manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks, the potential for rapid and widespread damage, CRA should act in a timely and co-ordinated manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate with the stakeholders accessing the CRA system, and implement procedures for rapid and effective co-operation with all concerned to prevent, detect and respond to security incidents. CRAs shall “respond’ by taking immediate steps after identification of an incident, anomaly or attack.

Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

The response and recovery plan of the CRA should aim at timely restoration of systems affected by incidents like cyber-attacks or breaches.

b. Recover

CRA shall “Recover’ from any cyber incident through incident management, disaster recovery and business continuity policies in place.

The recovery plan should be with reference to the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by the Board of the CRA as part of its IT infrastructure design, development and implementation.

Any cyber incident resulting in loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes. All such incidents shall be reported to PFRDA within 48 hours of the occurrence and detection of the event.

c. Reassessment

CRAs should review, reassess the security of information systems, networks, and make appropriate modifications to security policies, practices, measures and procedures at regular intervals or whenever any cyber incident takes place. New, changing threats and vulnerabilities shall be continuously monitored through appropriate channels and measures for protecting the systems from such threats shall be put in place. CRAs shall continually review, reassess and modify all aspects of security to deal with these evolving risks.

d. Fraud prevention controls

CRA shall take all measures necessary for prevention of all forms of fraud and including activities involving third-party’s or individuals who access the CRA system. It shall be the duty of the Risk Management and Audit Committees of CRA to review the findings of any internal investigations or internal audit or any other examination where there is suspicion of fraud or irregularity or a failure of internal control systems and report the matter to the board of CRA. The advice of the Board of CRA along with the complete information placed before the Board shall be reported to the Authority thereafter and as soon as practicable.

CRA shall immediately upon knowledge of occurrence of a fraud or if it has reason to believe that a fraudulent act has occurred, have a duty to promptly report such information to the Authority within 24 hours of such occurrence coming its notice and take appropriate action in line with the "PFRDA (Framework for Prevention and Reporting of Fraud Under NPS Architecture) Guidelines, 2023". CRA shall take all immediate actions to prevent further losses, whether monetary or otherwise including recovery of any losses resulting from fraudulent or corrupt activity using all means at its disposal, including civil or criminal legal action.

As part of the risk management related to fraud prevention, the following shall be put in place:

- Identify the systems or process that may have or have potential to facilitate perpetration of a fraud and put in place measures to plug the same.
- Initiate all actions necessary for recovery of losses caused to subscribers in the event of an incident.
- Identify the reasons for delay in detection including systems and procedures identified as the causative factors and plug the lacunae, and report to Risk Management Committee and Audit committee of the CRA.
- Ensure that staff accountability is examined at all levels in all the cases of frauds or alleged manipulation of CRA systems.
- Review the efficacy of the remedial action taken to prevent recurrence of any fraud, such as strengthening of internal controls.
- CRA shall endeavour to develop and improving it on a continuing basis of a fraud or suspicious transaction identification system for raising early warning signals whereby transactions are flagged for suspicious activity based on parameters to be identified by the CRA including alerts/signals based on their experience, client profile and business models.

Further, the Risk Management policy of the CRA shall deal with the following clearly so that the management, staff and all others who are discharging the duties and functions at CRA are aware of the controls. It shall be clearly understood that CRAs shall be responsible for any financial loss caused to subscribers due to the acts of omission or commission of its employees and agents in respect of conduct of its business including fraud.

Control Objective

It is defined as any action taken by management, the Board and other parties to enhance risk management and increase the likelihood that the established objectives and goals will be achieved. Control shall be incorporated to achieve the following objectives:

a. Safeguarding of assets

b. Effectiveness and Efficiency of operations

c. Accuracy and reliability of information

d. Compliance with applicable laws and regulations

i. Types of Controls

a) **Preventive** - Preventive controls are designed to prevent errors from occurring. Control occurs prior to processing the transaction.

b) **Detective** - Detective controls are designed to detect errors after they have occurred during processing.

ii. Control Nature

a) **Manual** - Performed manually by person in-charge of the control.

b) **Semi–Automated** - Manual controls that use computer-produced information.

c) **Automated** - Performed solely by the computer with no manual intervention.

iii. Control Categories

a) **Authorization** - Approval of transactions executed in accordance with applicable general or specific policies and procedures.

b) **Exception Reports** - Reports generated by the entity to monitor a violation of a set standard. CRAs shall devise exception reports by category of operations – subscriber contributions, demographic detail changes, Exits and Withdrawals, fund management, ASP related, nodal office or POP related, sector related (govt or corporate or voluntary etc).

c) **Configuration Controls** - Designed to prevent data against inappropriate processing by enforcing existence, accuracy, and presentation. Ex. building validation rules for the data being captured or processed.

d) **Segregation of Duties** - Separation of authority to prevent an individual to commit and conceal an error or an irregularity.

e) **System Access** - Ability of individual users to access a computer information system processing environment only as defined by the rights configured in that system. This shall include the access rules which govern the internal employees as well as external stakeholders.

f) **Interface / Conversion Controls** - Controls information transfers between 2 systems, whether automated or manual (sub-ledger to ledger) Ex: contribution receipts – Fund management systems, Inter CRA shifts, Exit and withdrawal module and subscriber registration and maintenance module etc.,

g) **Management review** - Activity of a person, different than the preparer, analysing and performing oversight of activities performed – Ex. Audit of transactions

h) **Reconciliation Control** - Designed to check whether two items / computer systems are consistent – No. of subscribers, contributions, AUM etc. generated from different systems. CRAs to identify all such sub-components of CRA system which have data from various sources and sub-systems to ensure that the data provided to the regulator or public or any stakeholder is consistent across for a given date.

iv. Some Key Controls

The following are some of the indicative key controls in relation to NPS accounts which shall be put in place. CRAs should examine the risk associated with each of the activity being performed and put in place controls in order improve quality, prevent any misuse of CRA system and occurrence of any fraud, whether leading to financial loss or otherwise.

a) **Change of Bank account –** Which shall surface any fraudster attempting to register bank account by producing tampered cheque copy or using the account other than of the subscriber or an attempted change where penny drop functionality fails due to name mismatch.

b) **Name mismatch -** At the time of redemption/pay-out, penny drop verification or other similar technology shall be compulsorily used to verify the name as available in the Bank vs in the CRA database. Any penny drop failure shall be reviewed and the processing of such redemption/pay-out shall be stopped immediately. Such penny drop failures shall be promptly brought to the notice of the concerned POP or nodal office. Redemption/pay-out shall be carried out only for those cases where the Penny drop is successful.

c) **Access to the system:** User creation for the CRA system shall be done by creating necessary request in online based tools. User privileges for internal uses to be provided on need-to-know basis and this will be reviewed on periodical basis and signed off by the respective department head. Also, the CRAs to ensure that subscribers/nodal offices/POPs/other stakeholders have privileges only to the extent that is required for them to operate the CRA systems for the desired objective.

d) **Password policy:** Change should be compulsorily enforced at pre-defined intervals and be made a complex one with numeric, special characters and alphabetical. A Password Policy duly approved by the risk management committee be put in place and concerning both internal users as well as the entire universe of external users. The CRA shall adopt a password policy that is consistent with emerging technologies, risks and practices of other market entities which are involved in providing financial services.

e) **2 Factor Authentication:** As far as possible, Access to the system to subscribers, nodal offices, Point of Presence or any other stakeholders shall be given using a 2-factor authentication – user id & password and OTP based. Additionally, access to CRA systems for Nodal offices or POPs can also be provided basing on the Aadhar based authentication service.

f) **Maker and Checker:** No activity shall be allowed to be performed without maker and checker in all systems or sub-systems of CRA. Checker activity should ideally be independent creation and matching of the maker data creation should be explored. Wherever systemic maker checker is not available, robust process should be in place, with appropriate audit framework to ensure effectiveness.

g) **Communication:**

- Sending the information related to change of bank account number by Email and SMS mandatorily. The consolidated information on such changes shall also be informed to the POP or the nodal office at the time of their login into the CRA systems on a weekly basis preferably in their dashboard or inbox
- Similarly, in case of any change in mobile number in a PRAN, SMS communication shall be sent to both the old mobile number as well as the new mobile number that is proposed. Further, along with the SMS, email communication shall also be sent to the registered email ID.

h) **Multiple PRAN** with the same Bank account number or mobile number shall be verified and not allowed to operate for any redemption/pay out including to explore any fraudulent bank account insertion.

e. Supplementary Risk Mitigation Measures

The following are some of the supplementary risk mitigation measures which are indicative and shall be put in place by the CRAs. They should examine the risk associated with each of the activity being performed and put in place similar risk mitigation measures in order improve quality, prevent any misuse of CRA system and occurrence of any fraud, whether leading to financial loss or otherwise.

Red Alerts:

This is a pro-active process to identify potential fraud and risk areas based on a pre-agreed combination of scenarios that happen in the PRAN (customer profile) through Financial Transaction (FT) / Non-Financial Transaction (NFT). All such qualifying cases shall be reviewed by Risk Management Team to ensure that there are no discrepancies. If any observation is noticed, then such instances are shared with the respective stakeholders for further action. Few of the indicative Red Alert scenarios are listed below and the CRAs should build red alerts based on their experience in dealing with the CRA systems and the concerned stakeholders including subscribers, nodal offices, point of presence etc:

- Change in bank account details in a PRAN more than once
- Changes in e mail/mobile more than once
- Requests for change in Date of Birth, Date of retirement, Name
- Withdrawals from dormant or inactive accounts.
- Withdrawals from account within a short time after changes in core details
- Logging into CRA system from a different city and from the city where the office is situated – This is only to keep a tab on the activity and need not be a show stopper.

Monitoring or examination of PRANs:

CRA shall monitor and specifically examine such PRANs where change of bank account, changes in demographic details had taken place and there is an Exit or withdrawal request (including partial withdrawals) made.

- Exit or withdrawal (including partial withdrawals) in a PRAN where change of Mobile Number has taken place prior to 30 days of initiation of Exit or withdrawal request including partial withdrawal.
- Exit or withdrawal (including partial withdrawals) in a PRAN where Change of Bank /Addition of Bank has taken place prior to 30 days of initiation of Exit or withdrawal request including partial withdrawals.
- Transactions (involving Exit or withdrawal including partial withdrawals) in a PRAN where there is a rejection by the nodal offices or Point of Presence (POP) in the last one year.
- Initiation of Exit or withdrawal request including partial withdrawals placed after nominee change within 30 days.

The CRA shall design and implement an efficient alert mechanism (SMS, Mail and physical communication(for important parameters including withdrawals)) to subscribers, nodal offices, POPs and other stakeholders whenever there is a request for a change in the demographic details including nomination or exit and withdrawal request is received or processed or contribution credit information for a PRAN is received in the CRA system.

CRA shall review such parameters from time to time to include any additional parameters for risk mitigation.

f. Quality policy

- CRA shall have a consistent and documented policy on quality assurance for all types of transactions that happen or occur in the CRA system and initiated by subscriber or a POP or a nodal office or any other stakeholder having access to the CRA systems. The policy on such quality analysis shall include Root Cause Analysis (RCA), modifications suggested in systems or processes in order to improve the quality of operations and transactions that are taking place in the CRA system.
- CRA shall analyse all the transaction types based on the policy put in place as part of the risk management policy.
- Risk Management committee and Audit committee shall be intimated on a quarterly basis on the findings of the quality analysis so conducted in the form of a detailed Quality Performance Review report by the Head of CRA operations.

g. Any other measure which aids the Risk management process.

- CRAs have vast experience in dealing with online systems and automated processes both under NPS space as well as other financial market related services. Accordingly, the CRAs shall basing on their past experience and evolving technological environment update the risk mitigation and management process on continuing basis. These measures can be over and above what has been stated above and with a aim to further strengthen the Risk management function at the CRA.

****