強制性公積金計劃管理局
MANDATORY PROVIDENT FUND SCHEMES AUTHORITY

電話號碼 Tel No	:	2292 1565
傳真號碼 Fax No	:	2259 8825
電郵地址 Email	:	
本局檔號 Our Ref	:	MPFA/S/TR/91/6(C)
來函檔號 Your Ref	:	

By Email

27 November 2019

Circular Letter: SU/CTR/2019/004

To: All Approved Trustees

Dear Sir/ Madam,

On-site Inspections on Data Risk Management, Cybersecurity Risk Management, Digital Readiness & Operational Efficiency

A good governance and an effective risk management are considered to be the key drivers to achieving better outcomes for scheme members, and approved trustees are expected to put in place an effective framework to manage different risks. In view of the rapid technological development and increasing usage of technology and data in the administration of MPF schemes, data and cybersecurity risks are two key risk factors that the approved trustees should take into account when evaluating and implementing their risk management processes /control measures.

To this end, the Authority has recently conducted on-site inspections to ten selected approved trustees focusing on the areas of data risk management, cybersecurity risk management, digital readiness and operational efficiency.

The key objectives of the on-site inspections are to (i) assess whether approved trustees have put in place effective governance framework and internal control measures over data risk management and cybersecurity risk management; and (ii) examine the current scheme administration processes and measures/ initiatives undertaken by approved trustees to enable digital readiness and enhance operational efficiency.

The review concluded that the trustees concerned have in general put in place the governance framework and control measures over data risk management and cybersecurity risk management and had undertaken different measures/ initiatives to promulgate the adoption of e-services. Nevertheless, there is still room for improvement in respect of trustees' oversight, control measures, employers and members' take-up rate and operational efficiency through digitalization. The trustees concerned are requested to undertake remedial actions. The key observations including the good practices from the on-site inspections are set out in **Annex.**

Approved trustees should review the existing governance and controls of their MPF administration in relation to the scopes of this review by making reference to the key observations from the on-site inspections and implement enhancement measures where appropriate. Notwithstanding, the approved trustees should be mindful that the key observations listed in Annex are by no means exhaustive and approved trustees should always take into consideration their own circumstances when implementing the relevant control measures.

Should you have any questions about the contents of this letter, please contact your supervisory manager.

Yours faithfully,

Ginni Wong

Ginni Wong
Director (Supervision)
Supervision Division

Encl.

Annex

1. Data risk management

1.1. Data accuracy

(a) Robust and effective controls to ensure data accuracy

In the course of the thematic review, the Authority observed that some trustees adopted stringent approach on data capture in order to minimize human input errors. For example, same set of data was required to be inputted by two different operational staff (i.e. double entry of data) and discrepancies found between the two sets of inputted data would be properly followed up before further processing the requests.

In terms of improvement area, approved trustees are expected to adopt more rigorous measures in monitoring and restricting the activities of operational staff who possess access right to directly create or modify members' data in the administration system. Adequate system controls should be put in place to prevent unauthorized changes/ creation of members' data in their scheme administration systems.

(b) Comprehensive data integrity review

Some trustees adopt a good practice whereby they engaged independent consultants to conduct comprehensive data integrity review with the aim of ensuring accuracy of members records maintained in the administration system and assessing effectiveness of data management system, controls on data management, detection of errors happened in members' accounts and remediation of adverse impact made to members' pecuniary interests. To better safeguard the interests of scheme members, approved trustees are highly recommended to conduct comprehensive data integrity review on a regular basis.

(c) Regular reconciliation of unit balance at member level

The Authority observed that a trustee adopts a good practice that it performed regular reconciliation of unit balance at member level. According to its practice, the closing balance of individual member account was reconciled against the opening balance and movement of all transactions of the particular constituent funds on a monthly basis. Approved trustees are expected to conduct regular reconciliation of unit balance at member level with the aim of ensuring data integrity.

1.2. Data patching

(a) Effective governance and controls over data patching process

In some occasions, the operational staff was not able to modify scheme/ members' data by using the existing built-in functions, the operational staff would raise a data patching request to IT department and such modification through back-end of administration system could override built-in validation controls pre-set in the system.

All data patching requests should be properly reviewed and authorized by all relevant stakeholders, such as, user department, IT, risk and compliance functions, before changes can be effected. Holistic impact analysis should be conducted to ensure that data amendments would not lead to any undesirable and unexpected impacts on other scheme administration data.

1.3. Change Management

(a) Established policies, procedures and controls over change management

The Authority observed in some cases that no comprehensive user acceptance testing or quality assurance checking was performed prior to the release of system enhancements which resulted in incorrect processing of members' requests. Without sufficient testing, system errors/ bugs relating to the system enhancements might not be timely identified.

To ensure adequate governance and controls over the system developments or enhancements processes, approved trustees are expected to, amongst other things –

- clearly define and document roles and responsibilities of each relevant parties involved in the change management process

- conduct impact assessment and comprehensive user acceptance testing where the changes involve critical system functions or it may cause potential impact to members' unit balances; and

- ensure that all change requests should be properly reviewed and authorized by all relevant stakeholders with proper evidences and audit trails.

1.4. Data disposal

(a) Effective monitoring and controls over data disposal

Approved trustees might outsource certain scheme administration functions/ tasks, such as, printing of members' statement, to their appointed external service providers whereby members' data/ transaction records have to be extracted or provided to them. Some trustees also provide members' MPF information to their servicing banks to facilitate member's enquiry via the bank systems, such as, online platform/ ATM. In one instance, the Authority noted no contractual agreement was established with servicing banks governing the use of data and the relevant data disposal requirements.

Approved trustees should put in place robust governance and controls to monitor the use and disposal of members' data by their appointed service providers or servicing banks. Further, it is crucial to clearly define the requirements on data handling, data disposal as well as other security measures to protect the members' data via establishment of contractual arrangements.

2. Cybersecurity risk management

2.1. Cybersecurity governance

(a) Effective cybersecurity governance and risk management

The Authority noted that most approved trustees placed reliance on their group companies for assessing and managing cybersecurity risk. However, individual cases revealed that the roles and responsibilities of monitoring and managing cybersecurity risk between the group companies and trustees were not clearly defined, and there was no active board-level involvement in formulating and implementing the overall cybersecurity strategy.

If there is a need to leverage resources from group companies, approved trustees should (i) establish policies and procedures to clearly define the roles and responsibilities in managing cybersecurity related risks and issues; and (ii) put in place sufficient monitoring controls to oversee the delegated activities/ services.

The board of approved trustees should have sufficient oversight of cybersecurity risk management by, among others, formulating cybersecurity strategies, conducting regular cybersecurity risk assessments, developing adequate cybersecurity capabilities and ensuring effective cybersecurity measures, so as to properly manage cybersecurity risk.

(b) Comprehensive review of the cybersecurity risk management framework by cyber expert

To enhance the cybersecurity risk management, it was observed that some trustees had proactively engaged external cyber experts to perform comprehensive review of their cybersecurity risk management framework which include, amongst other things, (i) inherent risk assessment of trustees' operations and (ii) maturity assessment of trustees' cybersecurity measures, in order to identify control gaps and areas for improvement.

Trustees are encouraged to leverage external expertise to enhance their cybersecurity risk management framework and conduct regular review to ensure effectiveness.

2.2. Cybersecurity controls

(a) Adequate cybersecurity capability to defend against different types of cyber-attacks

Most of the trustees implemented various cybersecurity controls to develop their technical capabilities for defending against a wide range of cyber threats, while the Authority also observed individual cases which merely relying on firewalls to defend against potential cyber-attacks or did not promptly implement complete measures to bridge the gaps identified in existing security capabilities with respect to new knowledge and threats.

Having regard to emerging cyber threats, approved trustees should evaluate the adequacy and effectiveness of their cybersecurity controls on a regular basis. Should there be gaps or deficiencies identified, approved trustees should establish a concrete implementation plan, with adequate resources, to promptly strengthen the relevant cybersecurity controls so as to ensure that they have adequate capability to detect and prevent different types of cyber-attacks in a timely manner.

(b) Reliable authentication mechanism in online platforms

All approved trustees provide online platforms for their scheme members to manage their MPF accounts. It was noted that some trustees had implemented two-factor authentication in their online platforms for users' login, while some simply applying passwords for user authentication. The Authority is concerned that single-factor authentication (e.g. passwords) may not be effective to prevent credential exploitation and other attempts to takeover users' account.

To better safeguard interests of scheme members, approved trustees should adopt stringent controls (e.g. multiple-factor authentication) to the authentication process in their online platforms to prevent unauthorized access to scheme members' accounts.

2.3. IT vendor management

(a) Up-to-date version of system components

The vendors of system components (e.g. operating system, database and application) release security patches (also called service packs), comprising a collection of updates, bug fixes or system enhancements, from time to time so as to protect the system components from viruses, malware and other sorts of cyber-attacks. Approved trustees should establish effective patch management procedures to ensure that security patches released by vendors are identified, assessed, tested and applied to relevant system components in a timely manner.

In general, vendors only provide security patches for each system component during the product life. It came to the Authority's attention in some cases that outdated system components were in use. Under such circumstance, no security patches would be available to detect and address system bugs and security vulnerabilities in their system components. To ensure the availability and continuity of security patches, approved trustees should monitor the product life of their system components and plan for system upgrade or replacement before the end of the product life.

3. Digital readiness and operational efficiency

3.1. Digital take-up

(a) Offering of digital tools to encourage employers and/or members to use e-services

With a view to offering better services to MPF scheme participants, approved trustees should deploy and promote the use of appropriate technology in delivering their MPF services. The Authority observed that majority of MPF trustees planned to introduce new digital tools (e.g. e-enrolment software, e-transfer via tablet) in order to encourage employers and/or members to use e-communications. Through the adoption of digital tools/ services, end-to-end straight through processing can be facilitated which has the advantages to (i) reduce manual input during data capture process which is prone to human error; and (ii) lower operating costs and achieve higher operational efficiency.

(b) Employers and members' digital take-up rates

Having said that, most of the trustees were observed with relatively low percentage of employers submitting remittance statement (RS) via electronic means. The cumbersome processes in handling paper RS and paper cheque payment jeopardize operational efficiency.

Besides, it was also noted that only low percentage of scheme members (~ 28% on average) had activated their online MPF accounts. Most of the scheme members even did not actively manage their MPF accounts via online platforms.

(c) Launch of publicity campaign or incentive programme to advocate the use of e-services

Approved trustees are encouraged to formulate publicity and education programme to promote the benefits of using digital channels for MPF account management and encourage scheme members to opt-in for receiving e-statements. It was observed that distributing leaflet or posting messages to official webpage were the most common methods adopted by trustees to promote e-services, while some trustees might also offer incentives to employers who make contribution via electronic means.

3.2. Operational efficiency

In the course of thematic review, a few trustees were observed with long processing time for various administration processes. The prolonged processing time was due to any of the following reasons:

- inefficient practice in handling payment via direct debit which the trustee concerned would only initiate the direct debit deduction in one batch on the 7th calendar day of the month following the relevant contribution period;
- long time pledge was agreed between trustee and its outsourced data processing centre; or
- long settlement period for the underlying investment funds of the scheme

It is highly recommended that approved trustees should review and re-design the relevant procedures or enhance the operational practices, where appropriate, with the aim of shortening the processing time and achieving operational efficiency.