

MANDATORY PROVIDENT FUND SCHEMES ORDINANCE (CAP. 485)

INTERNAL CONTROLS OF REGISTERED SCHEMES

## INTERNAL CONTROLS OF REGISTERED SCHEMES

### CONTENTS

	Page
1. Introduction	1
2. Reporting Requirements on Trustees	3
3. Internal Control Objectives and Suggested Control Measures	6
4. Reporting Requirements on Auditors	12
5. Exemption Arrangement for Employer Sponsored Schemes	14
Appendices	
A. Controls Relating to the Security of Scheme Assets	17
B. Controls Relating to the Compilation of Returns and Information to be Submitted to the Authority	20
C. Controls which Enable Compliance with Statutory Provisions	22
D. Controls Relating to the Separation of Scheme Assets	33
E. Controls Relating to Security of Data	35

## **1. INTRODUCTION**

### **1.1. Background**

1.1.1. The introduction of Mandatory Provident Fund (“MPF”) will bring into existence a formal system of retirement protection for Hong Kong’s workforce. MPF accrued benefits will be an important source in meeting scheme members’ financial needs after their retirement. It is, therefore, essential that a system of prudential supervision and regulation is in place to protect scheme members’ interests.

1.1.2. One of the effective asset security measures commonly adopted by financial regulators is the requirement of maintaining a proper internal control system. In this regard, the Mandatory Provident Fund Schemes (General) Regulation (“the Regulation”), Chapter 485A, imposes a statutory requirement on all registered schemes, except for certain employer sponsored schemes, in respect of the maintenance of internal control objectives and the establishment of relevant measures and procedures to achieve these objectives.

### **1.2. Purpose**

1.2.1. This Guideline is intended to set out:

- (a) the reporting requirements on trustees in respect of the internal controls of registered schemes;
- (b) the internal control objectives and suggested internal control measures in respect of registered schemes;

- (c) the reporting requirements on auditors in respect of trustees' internal control report; and
- (d) the exemption arrangement for certain employer sponsored schemes.

## **2. REPORTING REQUIREMENTS ON TRUSTEES**

### **2.1. General Requirements**

2.1.1. Section 39 of the Regulation requires each registered scheme to establish and maintain control objectives and internal control measures for achieving those control objectives at all times while the scheme is registered. Exemption is granted to certain employer sponsored schemes that satisfy prescribed criteria.

2.1.2. While section 39 of the Regulation does not specify who is responsible for maintaining the internal control objectives and measures, section 42 of the Regulation states that the trustee of a registered scheme will commit an offence for failure to comply with the requirements set out in section 39. Thus, even though approved trustees are allowed to delegate some of their duties to other service providers (such as scheme administrators, custodians and investment managers), the trustees must nonetheless ensure that proper controls are put in place, either by themselves or by the service providers they engaged, for the purpose of complying with section 39.

### **2.2. Reporting Requirements**

2.2.1. Under section 112 of the Regulation, an approved trustee of a registered scheme is required to submit to the Mandatory Provident Fund Schemes Authority (“the Authority”) annually a report on the scheme’s internal control objectives and major

procedures and measures for achieving those objectives. Where a trustee administers 2 or more registered schemes and the control objectives and measures applicable to those schemes are the same, the trustee may lodge a single report in respect of all those schemes. The report must be accompanied by an auditor's report.

### **2.3. Timing of Submission of the Report**

2.3.1. Section 112 of the Regulation states that trustee's internal control report, together with its auditor's report, must be submitted to the Authority within six months after the "relevant period". Section 111 of the Regulation provides that:

- (a) if the trustee is the approved trustee of only one registered scheme, the "relevant period" is the financial period of that scheme; or
- (b) if the trustee is the approved trustee of 2 or more registered schemes and a single internal control report is prepared for those schemes, the trustee shall nominate the relevant period as either the financial period of one of those schemes specified by the trustee or the financial year of the trustee and notify in writing to the Authority. Subsequent variation of relevant period is only permitted with the consent of the Authority.

2.3.2. To facilitate the Authority's monitoring of receipt of internal control reports, a trustee is expected to submit the nomination made under section 111(1)(b) of the Regulation on or before the

earlier of the ending date of:

- (a) the financial period of the registered scheme which will have the earliest financial period end date among all the registered schemes administered by the trustee and to be covered by the same internal control report; and
- (b) the financial year of the trustee.

### **3. INTERNAL CONTROL OBJECTIVES AND SUGGESTED CONTROL MEASURES**

#### **3.1. Introduction**

3.1.1. The Statement of Auditing Standards 300 “Audit Risk Assessments and Accounting and Internal Control Systems” issued by the Hong Kong Institute of Certified Public Accountants defines internal control system as being:

“all the policies and procedures (internal controls) adopted by the management of an entity to assist in achieving management’s objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information”.

3.1.2. This Guideline is not intended to prescribe specific control systems for all registered schemes. It mainly sets out the general objectives and major components of internal controls which are applicable to all registered schemes. It is recognised that a wide variety of internal control systems can be adopted to achieve the internal control objectives and different registered schemes may require different internal control systems. Furthermore, the suggested measures are not intended to be exhaustive and in many instances alternative control procedures will be equally appropriate and acceptable. Approved trustees

and auditors need to exercise their judgment in deciding whether a particular control measure is appropriate in a given circumstance.

### **3.2. Control Objectives**

3.2.1. Section 39(2) of the Regulation states that internal control system of a registered scheme must ensure that:

- (a) schemes assets are safeguarded in the interests of scheme members;
- (b) forbidden investments practices set out in the guidelines made by the Authority under section 28 of the Mandatory Provident Fund Schemes Ordinance (“the Ordinance”) are not contravened;
- (c) investments limitations and prohibitions imposed under the Regulation are complied with;
- (d) permissible investments as stated in sections 37(2), 51, 52 of and Schedule 1 to the Regulation are complied with; and
- (e) the funds of the scheme and the scheme assets are, except as permitted by the Regulation, kept separate from those of the participating employers, the scheme’s trustee, service providers and other persons appointed or engaged for the purposes of the scheme.

3.2.2. In connection with the compliance with the requirements under section 39(2)(e), an approved trustee is required to maintain books of accounts and other records as are necessary to separately identify the scheme assets so as to ensure the scheme

assets are distinct from the trustee's personal assets and from any assets held by the trustee for the benefit of a participating employer or any other person.

3.2.3. Besides the above objectives, an internal control system of a registered scheme should aim at providing reasonable assurance that:

- (a) operation of the scheme is planned and conducted in an orderly, prudent and cost effective manner;
- (b) transactions are entered into in accordance with governing rules of the registered scheme and with proper authority;
- (c) regulatory requirements as set out in the Ordinance and the Regulation are not contravened;
- (d) the accounting and other records of the registered scheme provide complete, accurate and timely information; and
- (e) customer and personal data security is adequately safeguarded.

### **3.3. Suggested Control Measures**

3.3.1. The following paragraphs set out internal control measures the Authority expects the internal control system of a registered scheme to cover. However, these measures are not intended to be exhaustive and the Authority may revise this guideline from time to time to take account of new developments and experience of the Authority and users. Other possible effective methods of achieving the above control objectives are equally acceptable. Trustees and auditors should take into account the circumstances

of individual schemes when assessing the adequacy of a scheme's internal control system.

- (a) Controls relating to the security of scheme assets: There must be adequate controls to ensure the security of scheme assets against loss due to irregularities, fraud or errors. Examples of key control measures are at Appendix A.
- (b) Controls relating to the compilation of returns and information to be submitted to the Authority: There must be adequate controls to ensure the accuracy and reliability of the information contained in statements, returns and reports submitted to the Authority. Examples of key control measures are at Appendix B.
- (c) Controls which enable compliance with statutory provisions: There must be effective monitoring and reporting systems to enable compliance with the Ordinance. These systems should be able to give sufficient advance warning to the trustee and service providers engaged by the trustee of situations which may lead to breaches so that appropriate remedial action can be taken. Examples of key control measures are at Appendix C.
- (d) Controls relating to the separation of scheme assets: There must be sufficient controls to ensure that books of accounts and other records are maintained as are necessary to separately identify the scheme assets so as to ensure that the scheme's assets are distinct from the trustee's personal assets and from any other assets of a participating employer or any other person. Examples of key control measures are at Appendix D.

(e) Controls relating to the security of data: There must be adequate controls to ensure the security of personal data as defined under the Personal Data (Privacy) Ordinance and customer data. Examples of key control measures are at Appendix E.

3.3.2. Even though trustees are not required to report on all the internal control measures applicable to their schemes, trustees are expected to ensure that a proper system of internal controls is in place for all aspects of their schemes' operation. The Authority is empowered under section 116(2) of the Regulation to direct trustees to rectify any deficiencies in the internal control measures of registered schemes, whether or not the Authority becomes aware of such deficiencies as a result of auditor's report under section 113 of the Regulation (see Chapter 4 below).

3.3.3 The control measures mentioned in paragraph 3.3.1(e) are expected to be incorporated into the internal control report for the financial year ending on or after 31 December 2010.

#### **3.4. Role of Internal Auditors**

3.4.1. Internal auditors of trustees and other service providers engaged by the trustees play an important role in monitoring the effectiveness of the internal control system of registered schemes. They should review and test the internal controls from time to time to ensure that they are functioning properly, and advise trustees or services providers on improvements and solutions to

problems. This is equally important in relation to those internal control measures that are not required to be reported to the Authority and reviewed by the external auditors under sections 112 and 113 of the Regulation.

3.4.2. If a registered scheme has an effective and independent internal audit function, external auditors are encouraged to liaise closely with the internal auditors in the planning and execution of their reviews under section 113 of the Regulation. Effective cooperation would help to minimize duplication of work depending on the extent the external auditors are satisfied with the scope, effectiveness and independence of the internal auditors' work.

## **4. REPORTING REQUIREMENTS ON AUDITORS**

### **4.1. Scope of Review**

4.1.1. Section 113 of the Regulation sets out the duty of auditor in respect of the report on control objectives and internal control measures which is required to be prepared by the trustee under section 112 of the Regulation.

4.1.2. Under section 113(4) of the Regulation, the auditor's report on the review must state the auditor's opinion as to:

- (a) whether or not appropriate control objectives were established and maintained for the scheme during the period to which the report relates;
- (b) if appropriate control objectives were so established and maintained, whether or not effective internal control measures were established and maintained for the purpose of achieving those objectives; and
- (c) whether or not those internal control measures (if any) were likely to have been sufficiently effective to provide a reasonable assurance that the control objectives established and maintained for the scheme would be achieved if those measures were fully and properly implemented.

4.1.3. For the purpose of section 113(4) of the Regulation, auditors shall consider the control objectives and internal control measures specified in the report prepared by the trustee in accordance with section 112 of the Regulation, review the report

and report in writing to the trustee in accordance with sections 113(4) and 113(5) of the Regulation.

4.1.4. Auditors are not expected to test or ascertain whether the control objectives or internal control measures were actually implemented during the period.

4.1.5. However, section 113(5)(a) requires an auditor to state, whether or not, during the course of the review of the trustee's internal control report, the auditor became aware of any shortcomings in the internal control measures that could materially affect the operation of the scheme (including its financial position) or the financial interests of scheme members.

4.1.6. In addition to reporting requirements with respect to report on internal control measures, auditors are also required to report to the Authority on awareness of matters stated in section 103 of the Regulation in the course of performing the auditor's duties and in accordance with the requirements specified in the same provision.

## **4.2. Auditing Guideline**

4.2.1. The Hong Kong Institute of Certified Public Accountants has issued the "Practice Note 860.1 The Audit of Retirement Schemes" to provide more specific guidance to auditors in the conduct of their work under section 113 of the Regulation.

## **5. EXEMPTION ARRANGEMENT FOR EMPLOYER SPONSORED SCHEMES**

### **5.1. Exemption Criteria**

5.1.1. The Regulation exempts an employer sponsored scheme from complying with sections 39 and 112 of the Regulation if the scheme has no more than 1,000 scheme members throughout the immediately preceding relevant period.

5.1.2. Alternatively, the Authority may grant an exemption if satisfied that:

- (a) for a substantial portion of the immediately preceding relevant period, the scheme had no more than 1,000 members;
- or
- (b) the scheme will not have, or is unlikely to have, more than 1,000 members during the current relevant period of the scheme.

5.1.3. For the purposes of sections 39(7)(a) and 112(6)(a) of the Regulation, the Authority will regard an employer sponsored scheme as having no more than 1,000 members for a “substantial portion” of the immediately preceding relevant period if the average number of scheme members at the end of each month was not more than 1,000 for at least seven months in the relevant period.

5.1.4. For the purposes of sections 39(7)(b) and 112(6)(b), an approved trustee has to submit the exemption application with the following information:

- (a) the number of scheme members as at the end of each month for the immediately preceding relevant period; and
- (b) grounds, with supporting evidence such as staff budget showing the expected number of staff for the current period, for believing that the scheme will not have, or is unlikely to have, more than 1,000 members during the current financial period.

The Authority will consider the merit of each application on a case by case basis.

5.1.5. It should be noted that exemption under sections 39 and 112 of the Regulation only exempt an approved trustee from maintaining a formal internal control system and reporting to the Authority in respect of the internal controls for the relevant employer sponsored schemes. The trustee will continue to have the responsibility of taking appropriate measures to ensure security of scheme members' interests and compliance with the MPF legislation.

## **5.2. Application Arrangement**

5.2.1. The exemption criteria for the purposes of sections 39 and 112 of the Regulation are the same. Trustees are therefore requested to submit their exemption applications under sections 39 and 112 of the Regulation together.

5.2.2. The Authority recognises that “immediately preceding relevant period” as stipulated in sections 39 and 112 of the Regulation does not exist at the inception of the MPF System. Under such circumstances, the Authority is ready to accept employee statistics provided by the sponsoring employers for the twelve months prior to the commencement of the schemes’ first relevant period as evidence for exemption application.

## Appendix A

### Controls Relating to the Security of Scheme Assets

#### I. Objective

There must be adequate controls to ensure the security of scheme members' assets against loss due to irregularities, fraud or errors.

#### II. Key Control Measures

To achieve the above objective, typical control measures which can be employed are:

- (a) There should be a proper segregation of duties in scheme operation. In particular, the functions of record keeping, authorisation and physical custody of scheme assets should be separated.
- (b) A system of authorisation for entering transactions should be established. Transactions exceeding the designated authorization limit can only be entered into with the prior approval of a higher level authority.
- (c) Transactions (such as the receipt and payment of contributions, accrued benefits and investments of scheme assets) should be recorded in a timely manner.
- (d) Trustee and service providers should discourage any money receipt or payment in respect of a registered scheme by cash and petty cash should not be maintained for a registered scheme.
- (e) No monies other than amounts received from scheme contributions, contributions surcharge, investment transactions or accrued benefits transferred from other schemes can be paid into the scheme's account.

- (f) Monies received for scheme must be paid without delay (within 4 bank trading days) into a bank account held on trust for scheme members after their receipt and trustee or service providers should require cheques payments to the scheme to be crossed and payable only to the trustee of the scheme.
- (g) Payment of scheme funds should only be made for valid benefit payments, transfer of accrued benefits of a scheme member from the scheme to another scheme, payments of the scheme's levies and administration charges and payments for investment transactions. There should be adequate procedures to ensure that any instruction for payments is bona fide and in accordance with relevant statutory requirements and payment cheques are crossed "Account Payee Only".
- (h) The trustee should establish and maintain appropriate and effective procedure in respect of transaction review process to prevent and detect errors, fraud and other improper activities. Preferably, an independent internal audit department should be established within trustee's and other service providers' organisations.
- (i) The trustee should make regular reconciliations of the trustee's internal records to those issued by third parties, e.g. statements from custodians, banks and investment managers, to identify and highlight for action any errors, omissions or misplacement of assets and such reconciliations should be reviewed by appropriate senior staff.
- (j) Reconciliations between total accrued benefits of each scheme member, each employer unit and the total assets held for the scheme should be made from time to time.
- (k) Scheme assets and other important documents such as cheque book and agreements are securely stored while they are in the trustee's or service providers' premises.

- (l) Use of standardised and sequentially numbered receipts and dispatch notes or other appropriate methods to acknowledge and account for scheme assets movements.
- (m) Appropriate controls exist with respect to access to computer systems to prevent unauthorized access for inputting, processing and retrieving computer data. Clear policies regarding confidentiality of passwords are developed e.g. passwords are regularly changed and relevant passwords disabled upon a staff member(s) leaving the trustee's or service providers' organisation.
- (n) Formal back-up and offsite storage procedures should be arranged for all computer files and key documentation.
- (o) The trustee and service providers should have a formal contingency plan in case of any disaster which will affect the scheme's operation.

## Appendix B

### **Controls Relating to the Compilation of Returns and Information to be Submitted to the Authority**

#### **I. Objective**

There must be adequate controls to ensure the accuracy and reliability of the information contained in statements, returns and reports submitted to the Authority.

#### **II. Key Control Measures**

To achieve the above objective, typical control measures which can be employed are:

- (a) There should be a procedure manual setting out the timing and method of compilation, source information used and other information gathering techniques which are necessary to ensure complete, timely and accurate preparation and compilation of statements, returns and reports and that changes in personnel will not affect the quality of the information submitted.
- (b) There should be clear documents/data for compilation of returns/reports to be submitted to the Authority to provide audit trails between the scheme's records and the returns/reports lodged with the Authority. Any material discrepancies between the records and the returns/reports submitted should be investigated and explained.
- (c) The approach and procedures used in the compilation of the returns/reports to be submitted to the Authority should be clearly understood by

the officers responsible for the preparation and checking. The guidelines and explanatory notes issued by the Authority for the purposes of preparing the returns/reports should be filed and kept up to date to facilitate future reference and make them available to the staff concerned.

- (d) In case of questions or uncertainty in compilation process, clarifications should be sought from the Authority and any results should be documented to facilitate future reference.
- (e) Prior to their submission, the returns and reports should be checked by a designated officer who takes no part in the actual preparation work.

## Appendix C

### Controls which Enable Compliance with Statutory Provisions

#### I. Objective

There must be effective monitoring and reporting systems to enable trustees and service providers to comply with their statutory duties under the Ordinance. These systems should be able to give sufficient advance warning to the trustees and service providers engaged by the trustee of situations which may lead to breaches so that appropriate remedial action can be taken.

While this is a general principle which applies to all provisions under MPF legislation, trustees and auditors will be asked to report specifically on those controls relevant to the compliance with:

- (a) guidelines made by the Authority under section 28 of the Ordinance with respect to forbidden investment practices; and
- (b) sections 37(2), 51 and 52, Part X of and Schedule 1 to the Regulation.

#### II. General Requirements

As a general principle, a trustee and the service providers engaged by the trustee should:

- (a) be aware of the relevant statutory provisions in the Ordinance;
- (b) keep up to date with changes in the Ordinance;
- (c) be aware of the guidelines issued by the Authority under sections 6H and 28 of the Ordinance and other communications from the Authority;
- (d) ensure that the information in (a), (b) and (c) above is filed and is

- communicated within the trustee's and service providers' organisations to those who need to be aware of it;
- (e) ensure that the above information is filed along with any specific rulings from the Authority communicated in writing or otherwise;
  - (f) ensure that they are fully aware of any transactions which could result in contraventions or potential contraventions of the Ordinance;
  - (g) ensure details of the procedures necessary to enable compliance with the various statutory duties should be documented in a procedure manual so that changes in personnel should not affect the trustee's or service providers' ability to comply with the requirement;
  - (h) ensure an officer is designated to monitor compliance. In case of doubt about the interpretation of the Ordinance, clarification should be sought with the trustee's or service providers' lawyer or with the Authority and the result of such clarification should be documented to facilitate future reference;
  - (i) establish an internal reporting and monitoring system to capture the appropriate source data from the accounting and other records in order to comply with any limitations set by the statutory provisions. The reports generated by the system should be reviewed by a designated officer on a timely basis;
  - (j) ensure clear, concise and organised working papers for monitoring compliance to provide audit trails for subsequent verification;
  - (k) ensure staff performing the compliance function possess the necessary skills, qualifications and experience to enable them to effectively execute their duties; and
  - (l) policies and procedures for proper handling of complaints are established and maintained and appropriate remedial action is promptly taken. The complaint procedures should be in writing. Where possible, complaints

should be investigated by staff performing the compliance function who are not directly involved in the subject matter of complaint.

Moreover, in order to ensure that service providers engaged by the trustee possess the necessary skills, qualifications and experience to enable them to comply with statutory duties under the Ordinance and duties delegated by the trustee, trustee should establish a formal policy setting out the selection criteria of service providers to be engaged by the trustee.

### **III. Specific Requirements**

In addition to the above common features, specific control measures should be installed in respect of the following:

- Capital preservation fund (section 37 of the Regulation)
- Repurchase agreements (section 51 of the Regulation)
- Securities lending (section 52 of the Regulation)
- Restricted investments (Part X of the Regulation)
- Permissible investments (Schedule 1 to the Regulation)
- Forbidden investment practices (guidelines made under section 28 of the Ordinance, no such guideline has yet been issued)

#### ***(a) Capital preservation fund (CP Fund)***

##### **Objective**

There must be adequate controls to ensure that the assets of the CP Fund are invested in secured instruments prescribed in section 37 of the Regulation, and administrative expenses are properly deducted in accordance with that section.

## **Key Control Measures**

To achieve the above objective, typical control measures which can be employed are:

- (a) The trustee should require the investment manager to provide periodic reports (e.g. monthly or quarterly report) relating to the investment portfolio of the CP Fund and check to ensure that it consists of investment types that are permitted by the Regulation and guidelines. In particular, the trustee should assign an officer to keep in view changes of credit rating of the invested debt securities to ensure that they meet the minimum credit rating requirement.
- (b) The trustee should maintain clear working papers for calculation of income and profit for investment and determination of the administrative expenses deductible from the CP Fund each month. These calculations should be independently checked and approved by senior personnel.
- (c) Officers of the trustee responsible for monitoring the CP Fund's operation should keep in view changes in the guidelines and other information issued by the Authority in relation to the CP Fund (e.g. class of authorised financial institutions and prescribed savings rate) to facilitate their monitoring of the CP Fund.

### ***(b) Repurchase agreements***

#### **Objective**

There must be adequate controls to ensure that the risk of loss of scheme assets resulting from repurchase agreement is minimised.

## **Key Control Measures**

To achieve the above objective, typical control measures which can be employed are:

- (a) A system of authorisation for entering into repurchase transactions should be established and details of all the proposed transactions should be reviewed by an officer of the trustee to ensure the transactions comply with the requirements before the transactions are entered into. If the trustee has delegated the authority to enter into repurchase agreements to the custodian, then the trustee should ensure that the custodian also has such an authorisation system.
- (b) If the trustee has appointed a custodian for a registered scheme and has, in the custodial agreement, delegated the authority to enter into repurchase agreement to the custodian, then the trustee should require the custodian to report from time to time on all the repurchase transactions entered by the custodian and should review the transactions to ensure they fulfill the requirements set by the Regulation and guidelines issued by the Authority.
- (c) An authorised list of eligible counterparties for entering into repurchase agreements must be in place and reviewed by the trustee regularly for credit risk. If the authority to enter into repurchase agreements has been delegated to the custodian, then the trustee must ensure that the custodian is kept informed of the updated list.
- (d) The basis to determine the margin requirement for different categories of debt securities based on their price volatility and other relevant factors should be clearly formulated, set out and updated in a manual by the trustee. If the authority to enter into repurchase agreements has been delegated to the custodian, then the trustee must ensure that the custodian

has a copy of the updated manual.

- (e) The trustee should have procedures to ensure adequate internal control measures in respect of repurchase agreements are in place. For example:
- different personnels are designated to check and mark-to-market daily the collateral in a repurchase agreement;
  - an independent personnel is responsible to conduct regular reconciliation of reports issued by counterparties, to identify and report omissions, errors or misplacement of assets and the reconciliation is checked and approved by senior staff.

If the authority to enter into repurchase agreements has been delegated to the custodian, then the trustee should require the custodian to report to the trustee on the procedures on internal control measures. He may, if he considers necessary, require the custodian to make appropriate improvements to these procedures.

- (f) The agreement between the custodian and the counterparties of the repurchase transaction should be documented and, where appropriate, reviewed by the trustee.

### ***(c) Securities lending***

#### **Objective**

There must be adequate controls to ensure that the risk of loss of scheme assets resulting from security lending transaction is minimised.

#### **Key Control Measures**

To achieve the above objective, typical control measures which can be

employed are:

- (a) A system of authorisation for entering into securities lending transactions should be established and details of all the proposed transactions should be reviewed by an officer of the trustee to ensure the transactions comply with the requirements before the transactions are entered into. If the trustee has delegated the authority for entering securities lending transactions to the custodian, then the trustee should ensure that the custodian also has such an authorisation system.
- (b) The trustees should require the officers responsible for monitoring the securities lending transactions to have a clear understanding on the policies set in respect of securities lending transactions and requirements under the Ordinance, Regulation as well as the guidelines issued by the Authority. If there is any uncertainty in the compilation process, clarifications should be sought and documented.
- (c) An authorised list of eligible counterparties for entering into security lending agreements should be in place and reviewed regularly by the trustee for credit risk. If the authority to enter into security lending agreements has been delegated to the custodian, then the trustee should ensure the custodian is kept informed of the updated list.
- (d) The basis to determine the margin requirement for different categories of debt securities based on their price volatility and other relevant factors should be clearly formulated, set out and updated in a manual so that the officers involved are fully informed of, and can make appropriate reference to the manual. A copy of the updated manual should also be sent to the custodian.
- (e) The trustee should have procedures to ensure adequate internal control measures for entering into securities lending transactions are in place. For example:

- different personnels are designated to check and mark-to-market daily the collateral in a security lending transaction;
- an independent personnel is responsible to conduct regular reconciliation of reports issued by counterparties, to identify and report omissions, errors or misplacement of assets and such reconciliation is checked and approved by senior staff.

If the authority to enter into security lending agreements is delegated to the custodian, then the trustee should require the custodian to report the procedures on internal control procedures. He may, if he considers necessary, require the custodian to make appropriate improvements on these procedures.

- (f) The trustee should establish a system on regular reports in respect of securities lending transactions. If the authority to enter into security lending agreements has been delegated to the custodian, then the trustee should require the custodian to provide periodic reports on securities lending transactions to review and check the calculations to ensure the transactions comply with the limitations set in the Regulation.
- (g) The agreement between custodian and the borrower of the securities should be documented and, where appropriate, reviewed by the trustee.

#### ***(d) Restricted investments***

##### **Objective**

There must be adequate controls to ensure that the limitations and prohibitions on restricted investments are not violated in accordance with Part X of the Regulation.

## **Key Control Measures**

To achieve the above objective, typical control measures which can be employed are:

- (a) In respect of an employer sponsored scheme, the trustee should always maintain an updated list showing all the participating employers and the associates of the participating employers of the scheme. A copy of that updated list should be sent to the investment manager. Whenever there is any change to the information on the list, the trustee should inform the investment manager of such change. This list should be confirmed with the participating employers at least twice a year.
- (b) The trustee should periodically review the reports prepared by investment managers to ensure that valuation of scheme assets is conducted on a regular basis to ensure that the stipulated limitations and prohibitions are not contravened.
- (c) The trustee should periodically review the details of scheme investments to ensure that the limits of investments in restricted investments are complied with.
- (d) The officer of the trustee who is responsible for monitoring restricted investments should keep up-to-date copies of all the guidelines and correspondence issued by the Authority on restricted investments.

### ***(e) Permissible Investments***

## **Objective**

There must be adequate controls to ensure that investment of scheme assets meets the permissible investment requirements stipulated in Schedule 1 to the

Regulation.

### **Key Control Measures**

To achieve the above objective, typical control measures which can be employed are:

- (a) The trustee should require the investment manager to establish a procedural manual for carrying out an investment transaction to ensure the requirements under the Ordinance, Regulation and guidelines issued by the Authority are not contravened. Examples in the procedural manual are:
- valuation of the scheme assets is conducted on a timely basis to ensure compliance with the stipulated requirements;
  - a staff officer is assigned to keep in view changes of credit rating of the invested debt securities so as to ensure that the minimum credit rating requirement is met; and
  - an independent personnel is responsible to conduct regular reconciliation of various reports, to identify and report omissions, errors or misplacement of assets and the reconciliation has to be checked and approved by senior staff.
- (b) A designated officer of the trustee should be assigned to periodically review the investment report prepared by the investment managers in respect of the investment portfolio of each constituent fund of the registered scheme. Random checking may be performed to ensure that the investments are in compliance with the requirements of permissible investments.
- (c) The trustee may require investment managers to provide periodic reports on their internal control system and measures in respect of investment of

the funds under the scheme to highlight if any actions are required or if any recommendations for improvements have been made.

- (d) The trustee should ensure that guidance in relation to investment of registered schemes issued by the Authority is filed properly (e.g. minimum credit rating requirement) for easy reference. He should also require the investment managers to establish and maintain a system for the proper filing of all the relevant investment requirements under the Ordinance, Regulation and guidelines issued by the Authority.

## **Appendix D**

### **Controls Relating to the Separation of Scheme Assets**

#### **I. Objective**

There must be sufficient controls to ensure compliance with the requirements in the MPF legislation relating to separation of scheme assets. In particular, books of accounts and other records are maintained as are necessary to separately identify the funds of the scheme to ensure that the scheme's assets are distinct from the assets of the participating employers, scheme's trustee, service providers or other persons engaged in the scheme.

#### **II. Key Control Measures**

To achieve the above objective, typical control measures which can be employed are:

- (a) Assets of the registered scheme for investment purposes are properly registered in the name of the scheme and documents of such investment assets are physically safe and secured, e.g. held by a custodian bank and that investment assets of the registered scheme are recorded separately from the assets of the participating employers, scheme's trustee, service providers or any other person.
- (b) Specific policies and effective procedures are established, maintained and followed to ensure sufficient independence of the investment manager and the custodian who holds the investment assets of the scheme.
- (c) Segregated bank accounts may be maintained for transactions of scheme's funds and the name of the bank accounts should make it clear that the

relevant registered scheme has ownership of the money held in the bank accounts. Opening of bank accounts should only be possible with the written authorisation of the trustee, or where there is a corporate trustee with the approval of the board of directors of the trustee. A majority of trustees or the board of directors in the case of a corporate trustee should approve in writing the signatories for each bank account.

- (d) Appropriate and effective procedures are established, maintained and followed to ensure contributions paid to the trustee in respect of the scheme are clearly identifiable as relating to the scheme. This may be achieved by means of specifying the payee as the trustee of the relevant scheme where payment is made by cheque or electronic means. The trustee should endeavour to discourage payments of contributions by cash.
- (e) Appropriate and effective procedures are established, maintained and followed to deal with unidentified remittances (e.g. payment without particulars of the person making the remittance). Unidentified remittances should be lodged in a suspense account which should enable the remittances to be separately recorded and readily identified.
- (f) The trustee should require reports (e.g. monthly statement) provided by service providers to clearly identify the assets of each scheme rather than a lump sum figures for all schemes operated by the trustee.
- (g) Reconciliations of assets held by different parties (e.g. custodians, investment managers and banks) and total assets for a registered scheme should be made regularly.

## Appendix E

### Controls Relating to Security of Data

#### I. Objective

There must be adequate controls to ensure the security of personal data as defined under the Personal Data (Privacy) Ordinance and customer data (generally referred to as “data”).

#### II. Key Control Measures

To achieve the above objective, typical control measures which should be employed include:

- (a) The trustee should develop policies and procedures to safeguard data security, particularly in relation to:
  - the granting of data access rights not to exceed the operational needs of different levels of staff;
  - the security of data stored in relatively less controlled peripheral equipment/devices such as portable storage devices and in paper form;
  - the handling of any cases of loss or leakage of data and the requirement to notify the Authority and affected customers of the incident and the remedial actions to be taken as soon as possible. If a large number of customers are affected, making a public announcement should be considered as this is an effective way to notify affected customers quickly and to regain their confidence by advising them of the remedial actions; and

- the compliance with the Personal Data (Privacy) Ordinance and any relevant codes of practice and guidelines issued by the Office of the Privacy Commissioner for Personal Data.
- (b) The trustee should set out their data security policies and procedures in a written document and notify all new staff to follow the policies and procedures and how to access them. The trustee should notify all staff as and when there is any change to the data security policies and procedures, and ensure that the staff have access to the updated policies and procedures. The trustee should also regularly remind all staff to follow the data security policies and procedures.
- (c) The trustee should periodically (at least annually) review compliance with data security policies and procedures, assess their effectiveness and, as and when necessary, enhance them.
- (d) Transfer of data from a centralized data facility to end-users' computer workstations for processing may increase the risk of leakage of data through users' internet email or portable storage devices connected to the workstations. The trustee should put in place adequate controls to limit the transfer of data in this manner. The trustee may consider controls such as removing the "downloading" facility in all computer workstations, or disabling floppy drives, USB ports, and Internet access of, computation workstations that have access to data. Control measures relating to data retrieval and downloading should be developed for regular review to identify irregularities. In addition, a regular review of user access rights and identity should be conducted. Both reviews should be conducted at a frequency of at least every 6 months.
- (e) The trustee should prohibit staff from downloading data from their computer workstations to portable storage devices (e.g. USB memory keys) unless there is a genuine operational need and with prior approval

from senior management. The data stored in such devices must be protected by data encryption and password, and the trustee should take reasonable steps to delete the data from the devices as soon as possible after use. Any loss of the devices should be immediately reported and investigated based on the policies and procedures established under (a).

- (f) There should be adequate controls to protect documents and other peripheral physical devices (e.g. tapes, USB memory keys) containing data and to ensure their security during transportation and in storage. These documents should be properly disposed of when they are no longer required by the trustee (e.g. shredding, erasure before disposal). Data stored in the peripheral physical devices should be encrypted. The trustee should consider installing, subject to surveillance laws and/or data privacy guidelines, appropriate surveillance systems in highly sensitive areas (e.g. document scanning areas, computer tape rooms, mailing rooms) to monitor unauthorized activities and to capture evidence for possible future investigation. The controls and procedures should also cover the documents and devices kept offsite.
- (g) If data is kept by outsourced service providers (e.g. outsourced scheme administrators, outsourced printers for the production of members' statements) or in offices located outside Hong Kong, the trustee should be satisfied as to the adequacy of data security measures put in place by these entities taking into account the standards laid down in this Appendix. Regular reviews as to whether the measures are being effectively implemented should be conducted. Data protection obligations and liabilities should be set out in the agreement between the parties including the service providers' agreement to ensure that such data security measures are in place during the term of engagement or appointment.