MANDATORY PROVIDENT FUND SCHEMES AUTHORITY

I.1 Framework for Regulatory Oversight of the Operation of an Electronic MPF System

TABLE OF CONTENTS

I. INTRODUCTION

Section 6E of the Mandatory Provident Fund Schemes Ordinance (Ordinance) provides for the functions of the Mandatory Provident Fund Schemes Authority (Authority). Pursuant to section 6E(1)(ec) of the Ordinance, the Authority is empowered to oversee the operation of an electronic MPF system, including (i) approving rules as described in section 19K(2)(a) of the Ordinance; (ii) giving to the System Operator and Approved Trustees directions or instructions the Authority considers appropriate for safeguarding the integrity and stability of the system; and (iii) monitoring the compliance with the Operating Rules and the directions and instructions mentioned in (ii) by the System Operator.

2. Pursuant to section 19K(2)(b) of the Ordinance, the System Operator must ensure that the electronic MPF system is administered and operated in a safe and efficient manner calculated to minimize the likelihood of any foreseeable disruption to the functioning of the system.

3. The Authority hereby sets out the oversight requirements in this framework (Framework for Regulatory Oversight) (a) as the Authority's directions and instructions to the System Operator under section 6E(1)(ec)(ii) of the Ordinance for safeguarding the integrity and stability of the eMPF Platform, and (b) for monitoring the compliance with the Operating Rules and the directions and instructions mentioned in section 6E(1)(ec)(ii) of the Ordinance by the System Operator under section 6E(1)(ec)(iii) of the Ordinance. In particular, this Framework for Regulatory Oversight is to explain the oversight requirements regarding the System Operator's duties under section 19K of the Ordinance and the processes that the Authority would follow in overseeing the eMPF Platform. For the avoidance of doubt, nothing in this Framework for Regulatory Oversight shall diminish or be in derogation of the duties and obligations of the relevant

parties, in relation to the eMPF Platform, under the Ordinance and its subsidiary legislation.

II. EFFECTIVE DATE

4. This Framework for Regulatory Oversight shall become effective on the date that the eMPF Platform is designated by the Secretary for Financial Services and the Treasury by notice published in the Gazette according to section 19I(1) of the Ordinance, i.e. 13 June 2024.

III. DEFINITION OF TERMS

5. Where a term used in this Framework for Regulatory Oversight is defined in the Ordinance or the subsidiary legislation then, except where specified in the Framework for Regulatory Oversight, the term carries the meaning as defined in the Ordinance or the subsidiary legislation.

6. Terms which appear in this Framework for Regulatory Oversight are defined as follows, except where expressly provided otherwise in this Framework for Regulatory Oversight:

(a) ***"API"*** means Application Programming Interface which is a computer programming approach for system-to-system data transmission in order to facilitate exchange of information and execution of instructions between different computer systems.

(b) ***"Approved Trustee"*** means a company or a natural person approved by the Authority as a trustee in accordance with section 20 of the Ordinance and, when used in relation to a registered scheme that is administered by two or more Approved Trustees, means (except in

sections 33 to 33B of the Ordinance) the trustees jointly and severally.

(c) ***"Bespoke Platform Customization(s)"*** means any modification or supplement to the eMPF Platform from time to time requested by an Approved Trustee and accepted and implemented by the System Operator in accordance with the terms of the Service Agreement in respect of the registered schemes managed by the requesting Approved Trustee.

(d) ***"Contractor(s)"*** means a person or persons from time to time engaged by the System Operator in respect of the performance of its activities or functions in respect of the eMPF Platform.

(e) ***"Data Protection Laws"*** means, in relation to each of the System Operator and the Approved Trustees, the PDPO and any relevant codes of practice, rules or guidance issued or approved by the Privacy Commissioner for Personal Data, and any other applicable laws relating to the use and Processing of Personal Data.

(f) ***"eMPF Platform"*** means the electronic MPF system (an electronic system designated under section 19I(1) of the Ordinance) and the Scheme Administration Services from time to time made available by the System Operator, as are more particularly described in the OR and the OM, and subject to any Bespoke Platform Customization applicable to an individual Approved Trustee, which may be accessed through the Service Centre and/or various electronic means by the Approved Trustees, their service providers, the participating employers and members, and other persons who are allowed access thereto.

(g) ***"IOPS"*** means International Organisation of Pension Supervisors.

(h) ***"MPFSGR"*** means the Mandatory Provident Fund Schemes (General) Regulation (Cap 485A).

(i) ***"OECD"*** means the Organisation for Economic Co-operation and Development.

(j) ***"OGCIO"*** means the Office of the Government Chief Information Officer.

(k) ***"Operating Manual (OM)"*** means the manual describing the scope and details of the Scheme Administration Services, relevant workflows and detailed operating requirements for the use of the eMPF Platform, as developed, issued and maintained by the System Operator from time to time in accordance with the OR.

(l) ***"Operating Rules (OR)"*** means the rules which have been made by the System Operator and approved by the Authority as mentioned in section 19K(2)(a) of the Ordinance.

(m) ***"Ordinance"*** means the Mandatory Provident Fund Schemes Ordinance (Cap 485).

(n) ***"PDPO"*** means the Personal Data (Privacy) Ordinance (Cap 486).

(o) ***"Personal Data"*** has the meaning given in the PDPO.

(p) ***"Processing"*** means, in relation to Personal Data, any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means

(q) ***"Scheme Administration Services"*** means the services and facilities from time to time made available by the System Operator to the Approved Trustees as described in the OR and OM.

(r) ***"Service Agreement (SA)"*** means, in relation to each Approved Trustee, an agreement entered into between the System Operator and

the Approved Trustee concerning the provision of the eMPF Platform by the System Operator to the Approved Trustee.

(s) ***"Specified Entity"*** means (a) the eMPF Platform Company Limited; or (b) a wholly owned subsidiary established under section 6DA of the Ordinance for the purposes of (i) facilitating the performance of the Authority's functions, and (ii) administering and operating an electronic system, and providing Scheme Administration Services for Approved Trustees, for the purposes of the new Part 3B of the Ordinance.

(t) ***"Staff"*** means a person or persons from time to time employed by the System Operator, the Contractor(s) or its / their subcontractor(s) in respect of the performance of the System Operator's activities or functions in respect of the eMPF Platform.

(u) ***"System Operator"*** means the Specified Entity that administers and operates an electronic system designated under section 19I(1) of the Ordinance.

(v) ***"Working Day"*** means any day other than (a) a public holiday; (b) a gale warning day or black rainstorm warning day as defined by section 71(2) of Interpretation and General Clauses Ordinance (Cap 1).

IV. OVERSIGHT STANDARDS

7. According to IOPS Principles of Private Pension Supervision[1], the objectives of private pension supervision focus on protecting the interests of pension fund members and beneficiaries, by promoting the stability, security and good governance of pension funds. In the global arena, pension regulations are increasingly focused on governance and risk management issues. Pension supervisory authorities around the world have also been following other financial sectors and moving towards a risk-based approach to pension supervision.

8. In January 2011, OECD / IOPS Good Practices For Pension Funds' Risk Management Systems[2] were published by OECD and IOPS. In particular, the good practices cover the main aspects of risk management systems in relation to pension funds, including governance arrangement, operational and outsourcing risks and controls, risk management mechanisms in terms of monitoring, reporting and communication.

9. In view of the international standards, the Authority has taken into account the objectives and relevant good practices in its formulation on the oversight standards on the eMPF Platform. The oversight standards are specified under respective requirement sections below, where the System Operator is required to comply with these requirements that the Authority considers appropriate for safeguarding the integrity and stability of the eMPF Platform on an ongoing basis. In particular, the oversight requirements for the purpose of complying with section 19K of the Ordinance are further elaborated under the

[1] IOPS Principles of Private Pension Supervision, https://www.iopsweb.org/principlesguidelines/IOPS-principles-private-pension-supervision.pdf

[2] OECD / IOPS Good Practices For Pension Funds' Risk Management Systems, http://www.iopsweb.org/principlesguidelines/46864307.pdf

relevant requirement sections. The Authority will regularly evaluate the System Operator against these requirements to oversee the operation of the eMPF Platform by the System Operator in administering and operating the electronic MPF system and delivering the Scheme Administration Services.

IV.1 Governance

10. Pursuant to section 19K(2)(b) of the Ordinance, the System Operator must ensure that the electronic MPF system is administered and operated in a safe and efficient manner calculated to minimize the likelihood of any foreseeable disruption to the functioning of the system.

11. In general, the System Operator should have proper governance arrangements that are clear and transparent, and promote safe and efficient operation of the eMPF Platform. In this connection, the board of directors and senior management of the System Operator should establish an effective oversight programme that includes (but not limited to) the following:

(a) clearly defined roles and responsibilities for administering, operating and monitoring the eMPF Platform;

(b) suitable parties with appropriate knowledge, skills and experience to fulfil their roles and responsibilities;

(c) development of a set of control policies (including, but not limited to, conflicts of interest policy, code of conduct policy) to ensure the eMPF Platform is administered and operated in a safe and efficient manner;

(d) adequate technical and other resources are appropriately allocated to support and monitor the operation of the eMPF Platform;

(e) proper management information systems to support effective management oversight;

(f) establishment of an effective risk management framework to ensure compliance with the control policies, OR, SA, as well as the directions or instructions given by the Authority as deemed appropriate; and

(g) ensuring the System Operator and Contractor(s) are competent to administer and operate the eMPF Platform, and adequate training programme is in place.

12. The System Operator should have in place an effective risk management framework, which includes its risk appetite and risk-tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in different contingency situations. The board of directors and senior management of the System Operator should determine an appropriate level of risk tolerance in relation to the operation of the eMPF Platform, and put in place policies, procedures and controls that are commensurate with the risk tolerance level. The governance arrangements should afford the risk management and internal control functions with sufficient independence, authority and resources.

13. The governance arrangements including the risk management framework should be properly documented and communicated to all relevant Staff and followed, and they should be subject to periodic review and approval by the board of directors and senior management of the System Operator.

IV.2 Safety

i. Reliability and robustness of the operation of the system

Performance Management

14. Performance objectives with respect to the reliability and robustness of the operation of the eMPF Platform should be clearly defined, where relevant policies are designed and established to achieve such objectives. Assessments should be performed regularly by the System Operator to assess the operation of the eMPF Platform against the established objectives.

15. The System Operator should identify the operational processes that are critical to the functioning of the eMPF Platform, where adequate performance monitoring should be performed over such processes. Arrangements should also be in place to support the detection of anomalies, frauds and incidents in these processes such that prompt actions can be taken against the risks posed by these activities.

16. As the eMPF Platform will probably process a huge volume of transactions, the System Operator should ensure that the eMPF Platform has adequate capacity for processing, in particular at peak times or on peak days. It should regularly monitor and test the actual capacity and performance of the eMPF Platform, and plan for capacity for growth due to changes in volumes or business patterns, so that the required processes for administration and operation of the eMPF Platform are maintained. Regular system capacity stress testing should also be conducted by the System Operator to verify whether the eMPF Platform can handle abnormally huge volume of transactions under extreme situations. If any deficiency in respect of the system capacity is identified, the System Operator should formulate remedial actions to resolve the issues of system capacity matters.

Business Continuity Plan

17. The System Operator should have in place a workable, well thought and fully documented business continuity plan to respond to and manage a crisis, and to ensure timely recovery and continuity of its operations in the event of a contingency. In general, this requires the System Operator to:

(a) conduct business impact analysis to identify different kinds of risks to business continuity and to quantify the impact of disruptions, including events that could cause a wide-scale or major disruption to the operation of the eMPF Platform;

(b) clearly define objectives (including recovery time and recovery points), policies and procedures that allow for the rapid recovery and timely resumption of critical operations following a disruption to a service;

(c) identify events that pose a significant risk of disrupting operations and establish mitigating measures to address such events;

(d) develop crisis and event management procedures in dealing with and containing an emergency to avoid spillover effects to the business as a whole, where the procedures should include procedures to deal with potential data loss and timely and effective communication strategies to consult with and inform all relevant parties (e.g. Approved Trustees), the Authority and others (e.g. critical service providers);

(e) establish an alternate site (i.e. recovery site) with appropriate network and infrastructure design, sufficient resources, capabilities, functionalities and appropriate staffing arrangements that would not be affected by a wide-scale or major disruption to the operations of the System Operator at the primary site and would allow the alternate site to take over the operations at the primary site if needed;

(f) undertake testing of its business and IT recovery arrangements regularly. The tests should include a range of scenarios of different nature, severity and duration relevant to its business and risk profile. Examples of scenarios that the System Operator may consider including, but not limited to, pandemics, natural disasters, and failures or disruptions at a third party or their supply chain. Relevant parties (e.g. Approved Trustees) and critical service providers, where appropriate and to the extent possible, should be involved in the testing; and

(g) conduct regular reviews of the adequacy and effectiveness of these arrangements and specify any gaps or weaknesses identified, as well as document the remedial actions planned.

Outsourcing Arrangements

18. Where certain operations of the System Operator are to be outsourced, it should ensure that the outsourcing arrangements will not impair the safety and efficiency of the eMPF Platform. The proposed outsourcing arrangements should be subject to a comprehensive risk assessment (including operational, legal, compliance and reputation risks) and that all the risks identified should be adequately addressed before launching the arrangements. In particular, the risk assessment should cover, among other things, the following:

(a) the importance and criticality of the services to be outsourced;

(b) rationales for the outsourcing (e.g. cost-benefit analysis); and

(c) the impact of the outsourcing on the System Operator's risk profile.

19. To manage the risk of outsourcing, the senior management of the System Operator needs to check if its Contractor(s) has / have proper financial

and technical capabilities to deliver the required services. This will be part of the due diligence and tender process before executing any written outsourcing agreement.

20. In any outsourcing arrangement, the senior management of the System Operator should retain ultimate accountability for the outsourced activity or function. An outsourcing arrangement can only allow the senior management to transfer its day-to-day managerial responsibility, but not accountability, for an activity or a function to Contractor(s). In this connection, the System Operator should establish effective control procedures to monitor the outsourced activities or functions.

21. The type and level of outsourced services to be provided and the contractual liabilities and obligations of the Contractor(s) should be clearly set out in an outsourcing agreement between the System Operator and its Contractor(s). Also, conditions for how the agreement can be terminated, and continuity / hand-over provisions need to be set out in the agreement. The System Operator should regularly (e.g. annually) review its outsourcing agreements, and it should assess whether the agreements should be renegotiated and renewed in view of changes in operational needs and external environment.

22. In any outsourcing arrangement, the System Operator should ensure that it has effective procedures for monitoring the performance of, and managing the relationship with, the Contractor(s) and the risks associated with the outsourced activities or functions. It should also establish reporting procedures which can promptly escalate problems relating to the outsourced activities or functions to the attention of the senior management, the Contractor(s), as well as to the Authority for those significant events. The control procedures over the

outsourcing arrangements should be subject to regular review by the System Operator.

23. If data is kept by Contractor(s) or in offices located outside Hong Kong, the System Operator should be satisfied as to the adequacy of data security measures put in place by these entities taking into account the control requirements laid down under section IV.2 iv. "Data protection and security" below. 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 Contractor(s)' agreement(s) to ensure that such data security measures are in place during the term of engagement or appointment.

24. Access to data by the Authority and the System Operator's internal and external auditors and parties who provide the third party assessment report, which is reasonably required, should not be impeded by the outsourcing. The System Operator should ensure that outsourcing agreement(s) with the Contractor(s) contain a clause which allows for inspection or review of the operations and controls of the Contractor(s) which are related to the outsourced activities or functions.

25. In order to ensure that the Contractor(s) engaged by the System Operator possess(es) the necessary skills, qualifications, experience and resources to enable it / them to comply with statutory requirements under the Ordinance and the subsidiary legislation and perform the obligations outsourced by the System Operator, the System Operator should establish a formal policy setting out the selection criteria of Contractor(s) to be engaged by it. The Contractor(s) should be required to observe all applicable confidentiality

requirements under the Ordinance (e.g. sections 41, 41A and 41B of the Ordinance) and the Data Protection Laws.

System Development and Change Management

26. On system development and change management, the System Operator should establish a general framework for management of major technology-related projects and system changes. This framework should, among other things, specify the eMPF Platform development and change management methodology to be adopted and applied. The methodology should cover, at a minimum, roles and responsibilities allocation, activity details, budget planning, impact analysis, risk assessment, milestones, check points, key dependencies, quality assurance and testing, approvals, post implementation verification and monitoring, and issue management. For any significant changes to the eMPF Platform (e.g. changes of the major functionalities of the eMPF Platform, changes with major impacts on the safety or efficiency of the eMPF Platform, etc.), the System Operator should notify the Authority before implementing the changes.

27. While unforeseen problems are to be addressed in a timely manner, the System Operator should establish formal procedures to manage emergency changes, including impact assessment, change approval, testing and post implementation review. In general, emergency changes may be triggered due to incidents that have caused or could cause an outage or significant degradation of the eMPF Platform, or for regulatory compliance issues. The System Operator should notify the Authority when emergency changes have been implemented.

28. Emergency changes should be properly logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible if necessary. Emergency

changes need to be reviewed by an independent personnel, who is independent of the actual change process from the segregation of duties perspective, to ensure that the changes are proper and do not have an undesirable impact on the production environment. Emergency changes should also be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.

Training

29. Since ensuring reliability and robustness of the operation of the eMPF Platform is important, there should be sufficient well-trained and competent personnel engaged in the operation. The personnel should possess appropriate level of knowledge and experience for their assigned tasks. Given the rapid pace of technological development, the System Operator needs to ensure that the Staff of technology functions, risk management functions and compliance functions, and internal auditors are competent and able to meet required levels of expertise and experience on an ongoing basis. The System Operator should ensure that staffing levels are sufficient to handle present and expected work demands, and to cater reasonably for Staff turnover.

30. To ensure that an adequate training programme is in place for the personnel, it is essential to establish a process to identify any material skill gaps of the Staff who are responsible for the key operation of the eMPF Platform. The System Operator may encourage and, where appropriate, facilitate its Staff, and should procure the Contractor(s) and its/their subcontractor(s) to encourage and, where appropriate, facilitate its/their Staff, such as those who are responsible for security management and risk management functions, to acquire relevant professional qualifications.

ii. Access control over the system

31. The System Operator should ensure the safety of the eMPF Platform by controlling access to the eMPF Platform's operation. The access to the eMPF Platform should be restricted by an adequate authentication mechanism associated with access control rules. Access control rules determine a user's rights and what functions, system resources and data the user can access. The user access should be periodically reviewed to mitigate the risk of unauthorized access.

32. Effective password controls should be implemented by the System Operator to ensure weak or easily guessed passwords are prevented and passwords are changed regularly. Stronger authentication controls (e.g. multi-factor authentication) should be adopted for higher risk transactions (e.g. payment) to ensure their integrity.

33. The use of and access to privileged accounts should be properly controlled, including (but not limited to) formal approval by appropriate management, monitoring of the activities performed by the accounts, stronger password controls and periodic review of the access granted.

34. When APIs are used to facilitate other parties to connect and access the eMPF Platform, appropriate access control configurations and measures should be deployed to prevent unauthorized access. The System Operator should carry out appropriate monitoring, identification, assessment, mitigation of fraudulent activities in relation to the usage of and access to APIs.

35. Separately, physical access controls are important to protect computer facilities and equipment from damage and unauthorized access. Comprehensive physical security policies that protect the eMPF Platform should be in place, where the policies are effective for supporting identification, assessment and mitigation of security threats and vulnerabilities at the physical sites that house the eMPF Platform and the associated infrastructure. The sites should be secured with proper security barriers and entry controls, and access permissions should be granted to authorized personnel only. Regular review on the access permissions should be performed to mitigate the risk of unauthorized access. Appropriate monitoring tools (e.g. surveillance camera) should also be utilised to support the physical security.

iii. Integrity of, and access control over, the information held within the system

36. Information integrity refers to the accuracy, completeness and consistency of information which ensure its fitness for use. The System Operator should ensure the integrity and confidentiality of data by adopting suitable measures and effective controls including (but not limited to):

(a) adequate back-up of all data and information within the eMPF Platform and regular back-up restoration tests;

(b) access to vital back-up records should be appropriately controlled;

(c) access controls over the system under paragraphs 31-35;

(d) data protection and security under paragraphs 37-40; and

(e) proper internal control mechanism to ensure data integrity.

iv. Data protection and security

37. Control procedures should be developed to safeguard application programs, operating systems, system software and databases. In particular, the System Operator should take into account all applicable confidentiality requirements under the Ordinance (e.g. sections 41, 41A and 41B of the Ordinance) in developing sound and robust policies and procedures on data security to protect data over the system, covering areas on, among other things,

(a) roles and responsibilities on data protection;

(b) management of security threats and vulnerabilities, including identification, assessment and remediation;

(c) secure control environment for data storage;

(d) logical and physical access controls;

(e) transmission of data, including data leakage detection and prevention; and

(f) management of data used by Contractor(s).

38. Where personal data are involved, the policies and procedures, including those to be followed by the Contractor(s), should also be in compliance with the Data Protection Laws. The System Operator should adequately implement security controls based on the developed policies and procedures.

39. The System Operator should set out its data security policies and procedures in a written document and require all its Staff, and should procure the Contractor(s) and its/their subcontractor(s) to ensure its/their Staff, to follow the policies and procedures and ensure they know how to access them. The System Operator should notify all its Staff, the Contractor(s) and its/their subcontractor(s)

as and when there is any change to the data security policies and procedures, and ensure that all Staff have access to the updated policies and procedures.

40. To protect the confidentiality of data, the System Operator should ensure a heightened awareness among Staff members in protecting the data. An effective awareness programme should be formulated by the System Operator to remind its Staff, the Contractor(s) and its/their subcontractor(s) periodically of the importance of complying with the data security policies and procedures, prompt reporting of potential leakage or loss of data (e.g. data of employers or scheme members) and the possible disciplinary actions for any violations. The policies and procedures on data security should be reviewed on a regular basis.

v. Record keeping

41. The System Operator should establish a set of policies and procedures on record keeping. The objective of the policies should be the creation and management of authentic, reliable and accurate, complete, and usable records which are capable of supporting Scheme Administration Services and activities of the System Operator. To achieve this, the System Operator should put in place a robust mechanism and appropriate controls to manage the data-related life cycle stages, typically including data capture, processing, retention, and disposal.

42. Scheme administration transactions and data (including but not limited to member enrolment, contribution processing, benefits transfer, fund switching, benefits withdrawal) should be captured accurately, completely and in a timely manner. Validations should be built into processes to minimize the risk of human errors as well as automated data feeds from external sources (e.g. Approved Trustees) so that data errors can be quickly identified.

43. Reconciliations between total benefits of each scheme member, each participating employer unit and the total assets held for a registered scheme should be made on each Working Day except a day on which the electronic MPF system is suspended under sections 19J or 19L(1)(a) or 19L(1)(b) of the Ordinance and the suspension affects the reconciliations.

44. Records should be stored securely and properly controlled according to the established policies and procedures. In particular, the System Operator should establish effective procedures to account for scheme assets movement and maintain adequate audit trails. Backup of records should be performed regularly. The policies and procedures on record keeping should also be reviewed periodically to ensure they are commensurate with business needs.

45. The System Operator should establish records retention and disposal schedules for its records to ensure systematic planning and orderly implementation of records disposal after records have been kept for the right length of time. In particular, the System Operator should observe the record retention requirement under the Data Protection Laws, and section 93 of MPFSGR, which requires that an accounting or other record required to be kept in respect of a registered scheme is kept for at least seven years after the end of the financial period for which the record is made or, if the record relates to a person's membership of the scheme, for at least seven years after the person ceases to be a scheme member. Such records may be kept in electronic form (where applicable) but should be readily accessible by the Authority for oversight and inspection purposes.

46. The System Operator should ensure that disposal of records should follow the established policies and procedures, and the disposal should be

properly authorized in advance by sufficiently relevant senior Staff in order to safeguard against premature disposal of records and destruction of records having archival value.

47. The System Operator should establish and maintain appropriate and effective procedures in respect of transaction review process to prevent and detect errors, fraud and other improper activities. The System Operator should keep abreast of the development of legal and regulatory environment that affects its record keeping arrangement, including but not limited to the Ordinance and the subsidiary legislation and the Data Protection Laws.

48. When the System Operator prepares information from its records and submits the information to the Authority, appropriate control measures should be employed to ensure the accuracy and reliability of the information. In particular, there should be proper procedures for compiling the information to ensure completeness, accuracy and timeliness of preparation. The System Operator should ensure that the procedures should be clearly documented, communicated to and understood by the Staff responsible for the preparation and checking.

49. The System Operator should implement quality assurance program to ensure the records are properly captured and kept according to the established policies and procedures. Identified areas of improvement should be enhanced accordingly.

vi. Risk management and control procedures relating to the operation of the system

50. The System Operator should put in place effective risk management and control procedures relating to the operation of the eMPF Platform. The senior management of the System Operator should establish clearly which unit(s) within the System Operator is / are responsible for implementing and managing the risk management process. Appropriate policies, procedures and controls should be used to identify, track and mitigate the relevant risks including but not limited to operational and technology related risks. The risk management process should be subject to periodic review.

51. While the established risk management unit is responsible for implementing and managing the risk management process, the unit has a role to assist business units and IT units in performing the risk management process that identifies, measures, monitors and manages operational and technology related risks. The risk management unit should also help identify, measure, monitor and manage the risks that relevant parties, such as parties who use or will have interface with the eMPF Platform, might pose to the operation of the eMPF Platform. Relatedly, the risk management unit should assist to identify, measure, monitor and manage the risks where operations might pose to other relevant parties.

52. Effective control measures should be put in place to ensure proper functioning of the eMPF Platform. In particular, the risk management unit should help to ensure awareness of, and compliance with, the System Operator's control policies, OR, SA, as well as the directions or instructions given by the Authority with respect to paragraph 11(f), and to provide support for investigation of any frauds and incidents, potential violations of any laws and statutory and / or

regulatory requirements. The risk management unit should be able to communicate freely to carry out its roles effectively. Separately, independent and risk-focused audits should be conducted by third line of defence on a regular basis to ensure the safety and efficiency of the eMPF Platform.

53. Adequate and comprehensive channels for the reporting and communication should be established, where internal control deficiencies, or ineffectively controlled risks, should be reported and communicated to the appropriate levels of management.

vii. Soundness of the system

54. A sound and robust security framework should be established by the System Operator to identify, respond to, and monitor security risks, including potential security vulnerabilities and threats, in relation to the administration and operation of the eMPF Platform. The security framework should be based on regular analyses of security risks of the eMPF Platform and conform to relevant standards (e.g. standards set by OGCIO). Monitoring of the security processes and compliance with the security framework should be performed on an ongoing basis.

55. In particular, given the evolving nature of cyber risks, an effective and comprehensive cyber resilience framework should be included as part of the security framework. The System Operator should identify its cyber risk exposure that it may face based on the type, volume, value and complexity of its operations. The relevant risks should be prioritized using a risk-based approach so as to locate threats that are pertinent to the eMPF Platform operation. Effective control procedures should be in place to guard against cyber attacks, including detection,

protection, recovery and response to cyber threats. As such, the System Operator should regularly assess the control procedures, test for vulnerabilities and ensure its resilience to relevant cyber risks.

56. Since cyber defence is important, the System Operator should conduct regular simulation exercises that have different attack scenarios to improve on the existing cyber resilience controls. The System Operator should monitor the trends in cyber threats, implement adequate measures to address different cyber-attack scenarios, and perform regular penetration testing and security assessments.

viii. Services provided to the system by the infrastructure associated with the system

57. The reliability and robustness of the operation of the eMPF Platform may depend on the continuity of services provided by the infrastructure associated with the eMPF Platform, where the associated infrastructure should be housed in data centers. The System Operator should identify, measure, monitor and manage the risks arising from the use of the services provided by the associated infrastructure.

58. Considering the communication networks transfer information and the provision of a channel of access to the eMPF Platform, proper safeguards including robust network design, well-defined network services and sound discipline should be observed by the System Operator. To prevent insecure connections to the System Operator's network, procedures concerning the use of networks and network services should be established, which cover authorization procedures, controls and procedures to protect network access, regular reviews of the parameter configurations of network related devices.

59. Given the importance of the infrastructure associated with the eMPF Platform, the System Operator should prudently consider the environmental risks that could affect adversely the operation of the associated infrastructure (e.g. fire, smoke, temperature, water, humidity and dust). A set of effective environmental controls should be in place to support monitoring and protecting the associated infrastructure. The associated infrastructure should also be protected from power outages and electrical supply interference by, for example, installing uninterruptible power supply.

60. Adequate access controls to the associated infrastructure should also be implemented to prevent unauthorized access. Regular inspections should also be performed by the System Operator to ensure that the access controls and environmental controls on the associated infrastructure are operating effectively.

ix. System is administered and operated in accordance with the Operating Rules

61. The System Operator should put in place effective control mechanisms to ensure that the eMPF Platform is administered and operated in accordance with the OR. Please refer to section IV.4 ii. "Monitoring of compliance with the OR" for more details.

IV.3 Efficiency

i. Speed and efficiency with which Scheme Administration Services are provided by the system

62. Pursuant to section 19K(4)(a) of the Ordinance, regard must be had in particular to the speed and efficiency with which Scheme Administration Services are provided by the eMPF Platform in determining whether the eMPF Platform is administered and operated in an efficient manner. In particular, the following requirements should be fulfilled:

(a) the System Operator should ensure that the eMPF Platform can process transactions in relation to Scheme Administration Services, including at peak times or on peak days, with the required speed. It should ensure the eMPF Platform's technical arrangements should be flexible to respond to changing demand and new technologies. In addition, the capacity for growth due to changes in volumes or business patterns should be evaluated by best effort, so that the required speed can be maintained;

(b) performance indicators (e.g. response time, transaction throughput, system availability and stability) should be defined to assess the efficiency of the Scheme Administration Services provided by the eMPF Platform. The System Operator should regularly test and monitor the performance of the Scheme Administration Services against the predefined indicators to ensure efficiency, including cost and fees consideration. The defined performance indicators should also be reviewed by the System Operator periodically;

(c) service levels should be defined by the System Operator to assess its performance in respect of its administration and operation of the eMPF Platform. The performance measurement should cover timeliness and quality of the Scheme Administration Services

provided by the System Operator. Each service level should be able to be measured objectively and reliably by the System Operator. The System Operator should regularly monitor, measure and report its achievement of the service levels to the Authority for review. The service levels should also be reviewed by the System Operator periodically; and

(d) the System Operator should also ensure the efficiency of operations, through periodically testing of the functioning of relevant internal control procedures so as to identify any enhancements with respect to the efficiency.

ii. Overall costs of the maintenance and operation of the system

63. Pursuant to section 19K(4)(b) of the Ordinance, regard must be had in particular to the overall costs of the maintenance and operation of the eMPF Platform in determining whether the eMPF Platform is administered and operated in an efficient manner. In general, the overall costs consist of the following elements:

(a) system maintenance costs – entail bugs fixing, performance improvement, functional enhancements, or any effort to keep the eMPF Platform running the way as expected; and

(b) system operation costs – associated with the administration and operation of the eMPF Platform on a day-to-day basis, which include the cost of resources used by the System Operator.

64. The System Operator should regularly monitor the overall costs of the maintenance and operation of the eMPF Platform to ensure cost efficiency with the efficient use of resources to achieve operation objectives.

IV.4 Operating Rules

65. Pursuant to section 19K(2)(a) of the Ordinance, the System Operator is required to make and put in place rules (i.e. OR) approved by the Authority governing the administration and operation of the eMPF Platform, and any suspension thereof. The OR are to stipulate the rules for operating the eMPF Platform to be adhered to by Approved Trustees and the System Operator, and prescribe rules for the (i) administration and operation of the eMPF Platform by the System Operator, and any suspension thereof; (ii) provision of Scheme Administration Services by the System Operator; and (iii) use of the eMPF Platform and Scheme Administration Services by the Approved Trustees to perform their scheme administration functions in respect of registered schemes.

i. Design of the rules

66. The OR should be clear, comprehensive and up-to-date. They should be consistent with the Ordinance and other applicable statutory and regulatory requirements, and provide an overview regarding the activities on administration, operation and suspension of the eMPF Platform. The OR should clearly indicate the roles and responsibilities of the Approved Trustees and the System Operator in the key scheme administration processes. The System Operator should inform the Approved Trustees of any amendments to the OR as approved by the Authority and provide reasonable notice of the implementation of such amendments to the Approved Trustees according to the mechanism set out in the OR.

ii. Monitoring of compliance with the Operating Rules

67. Pursuant to section 19K(2)(c) of the Ordinance, the System Operator must ensure that there are in place adequate arrangements to monitor and ensure

compliance with the OR, including arrangements regarding the resources available to the System Operator.

68. In particular, there must be effective monitoring and reporting mechanisms established by the System Operator to enable it to monitor and comply with the OR on an ongoing basis. These mechanisms should be able to give sufficient advance warning to the System Operator of situations which may lead to non-compliance with the OR so that appropriate remedial actions can be taken.

69. Where detailed procedures and manuals are established under the OR for particular areas of the operation of the eMPF Platform, effective control measures should be put in place by the System Operator to ensure that the underlying procedures and manuals are consistent with the OR at all times.

70. The System Operator should promptly notify the Authority of any failure of the System Operator and any Approved Trustees to comply with the OR which could pose risk to the administration and operation of the eMPF Platform.

iii. Arrangement to deal with addition, termination or restructuring of registered schemes and constituent funds

71. When the System Operator is notified about any registered schemes or constituent funds addition, termination or restructuring proposal, the System Operator should formulate an appropriate plan to respond to and deal with such situation in an orderly manner so as to ensure the operational resilience.

iv. Amendments to Operating Rules

72. It is the responsibility of the System Operator to ensure that the OR and any procedures or manuals established under the OR are in compliance with the Ordinance and the subsidiary legislation and other applicable statutory and regulatory requirements, having regard to any relevant guidelines issued by the Authority under section 6H of the Ordinance.

73. The System Operator may from time to time propose to amend the OR as it may consider necessary or desirable, while prior approval from the Authority should be obtained for any amendment to the OR. The System Operator should submit the following information to the Authority and any other relevant information as the Authority considers necessary for the Authority's consideration in relation to the proposed amendments to the OR:

(a) scope, details and reasons for the amendments;

(b) proposed effective date of amendments;

(c) risk assessment arising from the amendments and relevant risk mitigating measures; and

(d) impact on schemes, scheme participants and Approved Trustees.

74. Amendments to the OR should be communicated to Approved Trustees in the manner set out in the OR.

75. Separately, the Authority may give directions and instructions to the System Operator to amend the OR to ensure the eMPF Platform is administered and operated in a safe and efficient manner.

v. Suspension of the eMPF Platform

76. The System Operator may suspend the operation or use of all or any part of the eMPF Platform in the following circumstances:

(a) as directed by the Authority (section 19J of the Ordinance);

(b) for scheduled maintenance (section 19L(1)(a) of the Ordinance); or

(c) because of unforeseen circumstances (section 19L(1)(b) of the Ordinance).

77. The System Operator should inform the Authority as soon as practicable if suspension of the eMPF Platform is deemed necessary. Any scheduled maintenance should be carried out during non-peak hours as appropriate.

78. In the event of any suspension of the operation or use of the eMPF Platform (or any part thereof) pursuant to paragraph 76(a) above, the System Operator will publish information about the suspension in the manner the Authority considers appropriate.

79. The System Operator must publish information about the suspension of the eMPF Platform prior to suspending the operation or use of the eMPF Platform (or any part thereof) pursuant to paragraph 76(b) above and in accordance with the OR as required under section 19L(2) of the Ordinance.

80. In the event of any suspension of the operation or use of the eMPF Platform (or any part thereof) pursuant to paragraph 76(c) above, the System Operator must publish information about the circumstances giving rise to the need

to suspend the eMPF Platform (or any part thereof) and in accordance with the OR as required under section 19L(3) of the Ordinance.

81. The following information should be published:

(a) scope, details and reasons for the suspension;

(b) proposed period of the suspension;

(c) impact of the suspension; and

(d) remedial measures (if any).

82. The System Operator should have in place a robust business continuity plan to ensure timely recovery of all or any part of the eMPF Platform in the event of suspension. The System Operator should regularly update the business continuity plan and submit the updated plan to the Authority for review periodically.

V. OVERSIGHT APPROACH

83. The Authority has developed the oversight approach to continuously monitor and assess the compliance of the System Operator with the obligations imposed under the Ordinance and the subsidiary legislation. In particular, the Authority will monitor the System Operator's compliance with the OR, and the directions and instructions given by the Authority for safeguarding the integrity and stability of the eMPF Platform. The System Operator must ensure that the eMPF Platform is administered and operated in a safe and efficient manner. Following a risk-based approach, the oversight entails ongoing monitoring of the performance and effectiveness of the System Operator to comply with the requirements set out under section IV (Oversight Standards), focusing on areas of high risks that may have significant potential impact on the administration and operation of the eMPF Platform so as to facilitate early identification of issues and remediation. Where Scheme Administration Services are outsourced to Contractor(s) by the System Operator, the System Operator shall make sufficient and effective arrangement to facilitate the oversight role of the Authority in performing inspection or review of the operations, processes and controls of the Contractor(s) in relation to the outsourced activities or functions.

84. While the Authority is responsible for overseeing the System Operator, the primary responsibility for the daily operations of the System Operator rests with the System Operator itself. The Authority does not get involved in the daily operations of the System Operator.

85. The Authority will conduct the oversight of the System Operator through the following:

(a) on-site inspections;

(b) off-site monitoring, including interactions with the senior management of the System Operator;

(c) significant events / incident reporting; and

(d) third party assurance report.

V.1 On-site inspections

86. On-site inspections help the Authority to understand the operations, risk management and internal controls of the System Operator, and ensure the System Operator's compliance with statutory and regulatory requirements, as well as the requirements under the Oversight Standards. Inspections will be made on the basis of the Authority's decision, which will specify the subject matter and purpose of each inspection. While inspections are usually planned in advance, the Authority may conduct inspections in relation to an event or incident which requires immediate action.

87. In general, on-site inspections are conducted by using a risk-based approach, and efforts are prioritised where higher risks or lower level of controls are perceived within the System Operator. Higher risk areas will be generally subject to more frequent on-site inspections. The scope of on-site inspections may include (but not limited to) corporate governance, operational and technology risk management, business and continuity planning, and outsourcing arrangement. The inspection approach may consist of interviews, premises visit and inspection of relevant information and documents. Evidence is collected to ensure that an audit trail is in place for any weaknesses identified during the inspection.

88. The Authority will prepare an inspection report to set out the inspection findings. Before finalising the report, the Authority will discuss the identified findings with the System Operator so as to obtain its feedback for consideration. The report will then summarize the findings or concerns and make recommendations on remedial measures. The System Operator is required to rectify non-compliance issues and internal control weaknesses identified from these inspections within the timeframe specified by the Authority.

V.2 Off-site monitoring

89. Off-site monitoring, one of the oversight approaches to oversee the System Operator, forms the core of the Authority's oversight approach. Pursuant to section 19A of the Ordinance, the Authority has the power to require the System Operator to produce for inspection within such period (as may be specified in a written notice issued by the Authority) any record that is required to be kept under the Ordinance or is otherwise in the System Operator's possession or under its control.

90. Through off-site monitoring, information in relation to the eMPF Platform will be collected from the System Operator on a regular basis, which may include (but not limited to) business plans, control / risk management policies, resources arrangements, system performance statistics, transaction volumes, system changes, business continuity plan, complaints and related statistics, achievement of service levels.

91. The Authority may also require the System Operator to provide supplementary information, on a timely basis, for supporting off-site monitoring and other analyses. The information may include financial data of the System Operator, surveys, review on the quality assurance / compliance arrangement of

the eMPF Platform, risk management reports, internal or external auditor's reports and self-assessment related to the performance of the System Operator as required by the Authority.

92. Separately, the Authority maintains regular interactions (e.g. meetings) with the senior management of the System Operator to understand its operating model, latest plans and business initiatives, incidents, technology development, and the risks arising from such activities, with a view to identifying and assessing the risks associated with these activities in a timely manner.

93. The System Operator's prompt and accurate reporting of the aforementioned oversight information will contribute to the efficacy of the Authority's Framework for Regulatory Oversight. In this connection, the Authority would be in a better position to form a holistic view of the performance of the System Operator against the safety and efficiency requirements under the Oversight Standards. Any non-compliance with information requirements will warrant the Authority's close investigation and follow-up.

94. If the Authority becomes aware that there were deficiencies, errors, ineffective internal control measures, non-compliance issues, etc., the Authority may, by written notice to the System Operator, direct the System Operator to rectify the matters to the satisfaction of the Authority within a specified timeframe.

V.3 Significant event / incident reporting

95. As a general guidance, the System Operator should report to the Authority (i) any events which could, in the reasonable belief of the System

Operator, cause Approved Trustees to contravene the Ordinance or the governing rules of their registered schemes to the extent that the same are administered by the System Operator as part of the Scheme Administration Services provided by it pursuant to section 19K(1)(b) of the Ordinance; or (ii) any systems failures of the electronic MPF system referred to in section 19I(1) of the Ordinance which could, in the reasonable belief of the System Operator, affect the Approved Trustees' ability to perform their duties, that have come to the knowledge of the System Operator when it performs the Scheme Administration Services in response to the Authority's exercise of functions under section 6E(1)(ec) of the Ordinance or in compliance with any guidelines issued by the Authority under section 6H of the Ordinance.

96. In addition to the reporting obligation of the System Operator as mentioned under paragraph 95, the System Operator should report the following types of events / incidents in relation to Scheme Administration Services:

(a) events that are caused by the System Operator or the Approved Trustees leading to non-compliance with the OR or SA which may have a materially adverse effect (e.g. financial impact) to the interests of scheme members or could pose risk to the administration and operation of the eMPF Platform.

(b) breaches of other statutory and regulatory requirements not falling under paragraph 95, such as the Data Protection Laws and Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap 615).

(c) operational incidents which involve the following (but not falling under paragraph 95):

    (i) adverse financial impact on participating employers or scheme members;

(ii) incident that may attract attention in media or social media;

(iii) fraud and negligence, including fraud / misconduct of the Staff;

(iv) impact on a group of participating employers or scheme members;

(v) loss or leakage of data of a nature that may lead to material reputation risk to the System Operator, Approved Trustees and / or the Authority;

(vi) suspected or confirmed cyber attack that may cause potential loss or leakage of sensitive data (including, but not limited to, personal data) of the System Operator or the user of the eMPF Platform; or

(vii) breach of guidelines issued by the Authority under section 6H of the Ordinance or breach of directions or instructions given by the Authority under section 6E(1)(ec)(ii) of the Ordinance.

97. The System Operator should, not later than the third specified working day after becoming aware of the event or incident, report the event or incident to the Authority. The report should be prepared in writing, recapitulating the key facts, causes and impact of the event or incident being reported and the measures taken or to be taken by the System Operator in handling the event or incident.

V.4 Third party assurance report

98. On top of the oversight approaches by means of on-site inspection and off-site monitoring, the Authority may request the System Operator to submit

a third party assurance report that the Authority may require for discharging or exercising its functions, duties and powers under the Ordinance or the subsidiary legislation.

99. On a regular basis, the System Operator, or through its Contractor(s), is required to submit an independent auditor's assessment report on internal controls related to the control objectives (as stipulated under section 39 of the MPFSGR), applicable to the System Operator in performing Scheme Administration Services. The Authority may also require the System Operator to submit an independent auditor's assessment report on the requirements set out under sections IV.2 and IV.3 of this Framework for Regulatory Oversight. The assessment reports will facilitate the Authority in assessing whether the System Operator or Contractor(s) has / have implemented effective internal controls in discharging its duties in performing Scheme Administration Services and fulfilling the requirements set out under sections IV.2 and IV.3 of this Framework for Regulatory Oversight.

100. To supplement the oversight work of the System Operator, the Authority may also require the System Operator to submit a third party assurance report about any event or incident which could pose risk to the administration and operation of the eMPF Platform.

101. If necessary, the Authority may meet the auditors or parties who provide the third party assurance report together with the senior management of the System Operator to discuss the matters arising from the audit or third party assurance report.

V.5 Follow-up actions by the Authority

102. Pursuant to section 6E(1)(ec) of the Ordinance, the Authority is empowered to oversee the operation of an electronic MPF system, including giving to the System Operator and Approved Trustees directions or instructions the Authority considers appropriate for safeguarding the integrity and stability of the system. Accordingly, the Authority may provide recommendations to the System Operator to facilitate the System Operator to meet the requirements under the Framework for Regulatory Oversight, where appropriate. The System Operator should follow and act according to the recommendations as soon as practicable, while the Authority will closely monitor the implementation of the recommendations by the System Operator.

103. In case the System Operator refuses or fails to implement any of the recommendations within the timeframe as specified by the Authority, the Authority may consider giving a direction under section 6E(1)(ec) of the Ordinance to specify any action that needs to be taken by the System Operator within a specified period. For any situation where the Authority considers that it could pose risk to the administration and operation of the eMPF Platform (e.g. System Operator's non-compliance with a direction given by the Authority), the Authority may consider taking other actions (e.g. escalating the matters to the System Operator's board of directors) against the System Operator.