HONG KONG MONETARY AUTHORITY
香港金融管理局

PRACTICE NOTE

ON

SUPERVISION OF

STORED VALUE FACILITY

LICENSEES

June 2024

Structure

1. INTRODUCTION 1

2. PRINCIPAL BUSINESS AND FINANCIAL RESOURCES 2

3. CORPORATE GOVERNANCE 3

4. GENERAL RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS 15

5. INFORMATION AND ACCOUNTING SYSTEMS 16

6. MANAGEMENT OF FLOAT AND SVF DEPOSIT 17

7. SPECIFIC RISK MANAGEMENT 26

8. BUSINESS PRACTICES AND CONDUCT 55

ANNEX 61

1. Introduction

1.1. The Guideline on Supervision of Stored Value Facility Licensees (Guideline) issued by the Hong Kong Monetary Authority (HKMA) sets out the high level supervisory principles that the HKMA adopts in assessing the fitness and propriety of stored value facilities (SVF) Licensees. To help licensees in better understanding the standards by which the principles set out in the Guideline should be applied, the HKMA issues the Practice Note on Supervision of Stored Value Facility Licensees (PN) to provide additional guidance in respect of specific sections or paragraphs of the Guideline as and when necessary.

1.2. Licensees should regard this PN as illustrations of how a specific principle requirement can be met in typical situations. Licensees are expected to see through the illustrations and strive to achieve compliance with the Guideline by appropriately customizing their systems of controls, taking into account their specific situations. This PN should be read in conjunction with the relevant sections in the Guideline as well as relevant Frequently Asked Questions issued by the HKMA from time to time.

1.3. For the avoidance of doubt, the regulatory requirements on the SVF licensees are set out in the Payment Systems and Stored Value Facilities Ordinance and the Guideline. While this PN seeks to help licensees better understand how they may comply with those requirements, the PN does not have any effect of overriding or replacing any provisions in those documents.

1.4. For the sake of conciseness, this PN only includes sections or paragraphs of the Guideline on which additional guidance are provided. Going forward, the HKMA may revise existing guidance or issue additional guidance on other sections or paragraphs of the Guideline in the form of amendments to this PN as and when necessary. Owing to resources constraint, priorities will be determined based on the feedback from licensees and in view of their actual experience.

2. Principal Business and Financial Resources

Additional guidance will be provided as and when necessary.

3. Corporate Governance

Guideline section 3.2 - Corporate governance

Guideline 3.2.1	*A licensee is required to have in place sound governance arrangement for the purpose of effective decision-making and proper management and control of the risks of its business and operations. Such arrangement should include, among others, clear organizational structure with well-defined, transparent and consistent lines of responsibility. There should also be clear documentations on decision making procedures, reporting lines, internal reporting and communication process.*
Additional guidance	(a) As part of a sound governance arrangement, a licensee should put in place a code of conduct which lays down the standards of integrity and probity expected of its management and employees, and incorporates the relevant requirements under the PSSVFO concerning the fitness and propriety of its chief executive, directors and managers. The licensee should also have adequate systems for enforcing the code of conduct. (b) The adequacy and effectiveness of the governance arrangement and systems of risk management and internal control of a licensee should be subject to regular independent assessment in a risk-based manner. To determine the scope and frequency of such independent assessment, the licensee should perform self-assessment, at least on an annual basis, on key risk areas relating to its operation.
Guideline 3.2.2	*A licensee's board should be ultimately responsible for the sound and prudent management of a licensee's SVF business operations. As such, the responsibilities, organization, functioning, and composition of the licensee's board of directors must be clearly defined and documented.*
Additional guidance	(a) While a licensee's board should determine its structure, composition, and terms of reference, to ensure sound and prudent management of a licensee's SVF business operations, the

typical responsibilities of a board include but not limited to the following:

(i) Set the objectives, risk appetite, and corporate values of the licensee and approve strategies for achieving those objectives while staying within the risk appetite and upholding the corporate values;

(ii) approve key policies to establish strong risk governance and effective system of controls such that the operation of the licensee is conducted in a safe and efficient manner through the adoption of sound and prudent practices;

(iii) oversee the performance of senior management staff with a view to ensuring that they exercise their duties in accordance with approved policies and exercise their duties within delegated authorities; and

(iv) ensure that key control functions, including but not limited to operational and IT risk control, compliance, internal audit and external audit, are effectively in place with sufficient independence from business units.

(b) The Board should have in place appropriate policies and procedures to regularly assess the ongoing suitability of the board members, taking into account all relevant factors such as but not limited to competence, performance in relevant board and committee discussions and/or deliberations, and whether potential conflict of interest is properly mitigated on an ongoing basis by putting in place appropriate systems of control.

Guideline 3.2.3	*The board should have an adequate number and appropriate composition of members to ensure sufficient checks and balances and collective expertise for effective, objective decision-making. The size and composition of the board will vary from institution to institution depending on the size and complexity of the licensee and the nature and scope of its activities. As a general benchmark for demonstrating sufficiency of checks and balances, normally one-third of their board*

	members should be independent non-executive directors (INED).
Additional guidance	(a) In situations in which a licensee can demonstrate to the satisfaction of the HKMA that its structure and circumstances render it very difficult or ineffective to comply strictly with this guideline, the HKMA may consider accepting alternative arrangement that has the same effect of ensuring sufficient checks and balances and collective expertise in the board. (b) In considering the eligibility and suitability of a person to be (or continue to serve as) an INED, the licensee should, among other things, assess whether such person has the necessary independence. Examples of relevant assessment factors include: (i) the person's shareholdings or financial dealings, if any, in the licensee or its shareholder controllers as defined in the PSSVFO, group companies, or subsidiaries; (ii) whether the person has recently been an employee, executive or director (other than INED) of the licensee or any of its shareholder controllers as defined in the PSSVFO, group companies, or subsidiaries; (iii) whether the person has any material business relationship with, or receives any significant compensation from, the licensee or any of its shareholder controllers as defined in the PSSVFO, group companies or subsidiaries, except for remuneration for service as an INED; (iv) whether the person has any close connections with the licensee or any of its shareholder controllers as defined in the PSSVFO, group companies or subsidiaries; (v) whether the person holds any other capacity that might give rise to conflict of interest, such as but not limited to having material links with other directors of the licensee. (c) The licensee should ensure that an INED shall neither be part of its executive team nor engage in its day-to-day management,

including but not limited to its management-level committee.

Guideline 3.2.5	*Whilst the board is ultimately responsible for the overall soundness of a licensee, the appointment of competent management is key to achieving the objective of a soundly and efficiently run licensee. The board works with a senior management team (senior management) to achieve this and senior management remains accountable to the board.*
Additional guidance	(a) As set out in the additional guidance for Guideline 3.2.2, the board in discharging its duties can delegate appropriate authorities to a senior management team, but effective arrangement should be put in place such that the board can assess the performance of the senior management and to hold them accountable in case of less than satisfactory performance. (b) The board should actively engage in succession plans for the chief executive and other key senior executives as appropriate.

Guideline 3.2.6	*Senior management are responsible and accountable for running the business of a licensee effectively and prudently in accordance with the business strategies, policies, risk appetite, as well as delegation of authorities set down by the board.*
Additional guidance	(a) In general, the senior management team should be responsible for, among others, the following: (i) Propose business plan, policies, key performance indicators, and risk limits for deliberations and approval by the board; (ii) Develop a robust system of controls which typically comprise, among other things, proper segregation of duties, clear allocation of responsibilities and delegation of authority, adequate internal checking and reconciliation, an effective and timely IT system and management information system, a robust staff recruitment, development and appraisal program, and an independent internal audit and compliance function; and (iii) Formulate an effective risk management framework for

managing different aspects of risk arising from the licensee's business activities, based on the business strategies, risk appetite and policies approved by the board.

Guideline section 3.3 - Fitness and propriety of officers and controllers

Guideline 3.3.2	***Directors and chief executives*** *Given the leadership role of directors and chief executives, fitness and propriety will be assessed taking into consideration of their integrity and competence, which will generally be assessed in terms of relevant knowledge, experience, judgment as well as leadership. Their commitment and ability to devote sufficient time and attention to the SVF business will also be assessed. The standards required of persons in these respects will vary considerably, depending on the scale and complexity of a licensee's operations.*
Additional guidance	(a) In evaluating the integrity of a person, the HKMA will generally review whether there are any records, incidents or issues that may cast doubt on the honesty and integrity of that person. While an exhaustive list is impossible, below are typical scenarios in which a person will need to demonstrate to the satisfaction of the HKMA that those scenarios do not cast doubt on the person's honesty and integrity: (i) the person who has been subject to a disciplinary action (e.g. reprimand, fine, suspension of licence) by any regulatory authorities or professional bodies; (ii) the person has been convicted of a criminal offence; (iii) the person is an undischarged bankrupt, is currently subject to bankruptcy proceeding, or has bankruptcy history; (iv) the person is found by a court or other competent authority for fraud, dishonesty or misfeasance; (v) the person has a record as a controller, chief executive,

director or manager of a corporation or business that was wound up or insolvent; and

(vi) the person is refused or restricted from the right to carry on any business or profession for which a specific licence, registration or other authorization is required by law.

(b) In evaluating the competence of a person, the HKMA will consider a person's industry experience, management experience, academic and professional qualifications, knowledge in SVF operation and products, and regulatory knowledge. The HKMA will also review whether there are any records, incidents or issues that may cast doubt on the competence or leadership of that person. While an exhaustive list is impossible, below are typical scenarios in which a person will need to demonstrate to the satisfaction of the HKMA that those scenarios does not cast doubt on the person's competence:

(i) the person has been disciplined by a professional, trade or regulatory body for incompetence, negligence or mismanagement;

(ii) the person has been dismissed or requested to resign from any position or office for negligence, incompetence or mismanagement;

(iii) the person is an undischarged bankrupt, is currently subject to bankruptcy proceeding, or has bankruptcy history;

(iv) the person has a record as a controller, chief executive, director or manager of a corporation or business that was wound up or insolvent; and

(v) the person is refused, restricted or suspended from the right to carry on any business or profession for which a specific licence, registration or other authorization is required by law.

In considering such cases, the HKMA will take into account factors

such as the nature and seriousness of the event, the roles and responsibilities of the person concerned in the event, and actions taken or improvements made by the person concerned since the occurrence of the event. The HKMA will request the person concerned to explain why those records, incidents, or issues do not suggest lack of competence or what have been done since then to enhance the person's competence level.

(c) In considering whether the relevant person could devote sufficient time, attention and effort to the SVF business, the HKMA will review a number of factors including but not limited to whether the person has other management and/or executive roles or directorship in other companies, and if so the business nature of such companies. Further, directors should make every effort to attend all the meetings of the licensee's board of directors and any committees which he or she sits.

Guideline 3.3.3.1	***Controllers*** *In assessing the fitness and propriety of controllers, a key consideration is the influence that a controller could potentially have on the interests of the users and potential users of the scheme concerned. This has to be assessed in the context of the circumstances of individual cases. The general presumption is that the greater the influence on the licensee, the higher the standard will be for the controller to fulfil the criterion. Willingness and ability to work collaboratively with other controllers and the management team will also be a key factor of consideration.*
Additional guidance	(a) Factors to be considered in assessing the potential influence of a controller applicant on a licensee include: (i) the level of shareholding as proposed by the applicant, as compared to other existing shareholder controllers, (ii) the number of directors to be nominated to represent the applicant, (iii) intention of the applicant seeking to become a controller,

e.g. to maintain status quo or to initiate significant changes to the business strategies or setup of the licensee; and

(iv) presence of any written agreement or commitment, e.g. commitment not to influence the business strategies of the licensee.

Guideline 3.3.4.1	***Managers*** *Similar principles as set out for directors and chief executives will be applied for assessing the fitness and propriety of managers, but assessment will be made in the context of the specific businesses or control areas of the managers. Pursuant to section 3(3) of Schedule 3 to the PSSVFO, a licensee should have in place appropriate and adequate systems of control to ensure that each of its managers is a fit and proper person to hold the position concerned.*
Additional guidance	(a) An appropriate and adequate system of control for the purpose of ensuring the fitness and propriety of managers of a licensee would typically feature the following: (i) that all positions which fall within the definition of "manager" as set out in the PSSVFO are identified in a proper and timely manner; (ii) that the responsibilities of, and the skills, knowledge and experience required for, individual managerial positions are clearly defined and supported by up-to-date job descriptions, organisation charts and levels of authority; (iii) that there are in place proper policies and procedures for selecting and appointing managers and for satisfying the licensee itself about the fitness and propriety of candidates with due regard to the position that the person holds or is to hold; (iv) that there are in place effective systems to appraise, reward and discipline managers in accordance with their performance and to evaluate their fitness and propriety on

a regular basis;

(v) that there are in place policies and procedures for investigating breaches of rules and regulations by managers or complaints against them and the resultant disciplinary actions;

(vi) that managerial vacancies are filled promptly and there are clearly defined arrangements to provide cover in the case of temporary vacancies;

(vii) that adequate training is provided to managers; and

(viii) that the systems of control in relation to the appointment of managers are subject to periodic review by the internal audit function.

Guideline section 3.4 – Outsourcing

Guideline 3.4.3	*When outsourcing any of its operations or functions, a licensee should (a) properly plan for the outsourcing arrangements by conducting a comprehensive risk assessment to identify and evaluate all risks involved and structuring the outsourcing arrangements to ensure that all material risks identified (including business interruption risk) have been adequately managed before launch and that the outsourcing arrangements will not impair the effectiveness of its internal controls or compromise the interest of the SVF users; (b) properly implement the outsourcing arrangements by performing appropriate due diligence on the service providers, conducting appropriate testing to ensure that the services to be rendered fully meet the agreed performance standards, executing appropriate outsourcing agreements with the service providers to set out clearly the outsourcing arrangements and the related rights and obligations, and carrying out proper transfer of the related operations or functions to ensure smooth transition; and (c) properly manage the outsourcing arrangements on an on-going basis by performing appropriate regular quality review of the outsourced operations or functions to ensure that the services being rendered continue to meet the agreed performance standards in full and all*

	deficiencies identified are duly rectified, conducting appropriate regular risk assessment to ensure that all material risks are duly identified, evaluated and adequately managed on an on-going basis, and reviewing the outsourcing agreements at appropriate intervals to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in the licensee's business strategies.
Additional guidance	(a) Typically, appropriate due diligence conducted for a service provider should take into account, apart from the cost factor and quality of services, the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity to meet the licensee's demand in the longer run, familiarity with the payment industry, and capacity to keep pace with innovation in the market. (b) Typically, an appropriate outsourcing agreement should set out clearly (a) the type and level of services to be provided and the related performance standards of the service provider, including its contingency arrangements in respect of daily operational and systems problems; (b) the contractual obligations and liabilities of the service provider; and (c) the rights and obligations of the licensee including the relevant fees and charges payable by the licensee and the rights of the licensee to access, retrieve and retain in Hong Kong on a timely basis accurate and up-to-date records and make those records available for inspection by the relevant authorities including the HKMA, if required; and (d) data handling controls such as storage, backup, protection and confidentiality and data removal arrangements upon termination or expiry of the contract. (c) In a typical situation, business interruption risk in respect of outsourcing arrangements could be addressed by means of contingency arrangements. Contingency arrangements in respect of daily operational and systems problems would normally be covered in the service provider's own contingency plan. Typically, a licensee should ensure that it has an adequate understanding of its service provider's contingency plan and

consider the implications for its own contingency planning in the event that an outsourced service is disrupted due to failure of the service provider's system[1]. Such contingency plans should be tested by the licensee and its service providers regularly where practicable.

(d) In relation to overseas outsourcing, the following matters should typically be addressed in the outsourcing arrangement in addition to those considerations set out above:

(i) Implications of the overseas outsourcing for licensee's risk profile;

(ii) Right of access to users' data by overseas authorities such as the police and tax authorities (a licensee should notify the HKMA if overseas authorities seek access to its users' data);

(iii) Notification to customers;

(iv) Right of access to users' data for examination by relevant Hong Kong authorities including the HKMA after outsourcing; and

(v) Governing law of the outsourcing agreement.

Guideline 3.4.4	*A licensee should ensure that its outsourcing arrangements comply with the Personal Data (Privacy) Ordinance ("PDPO") and any relevant codes of practice, guidelines and best practices issued by the Office of the Privacy Commissioner for Personal Data ("PCPD") from time to time.*
Additional guidance	(a) Typically, a licensee could ensure such compliance by putting in place effective measures to ensure that all applicable legal and regulatory requirements under the PDPO are properly observed by the service providers, in particular, notifications to or seeking of consents from users are properly carried out and records of

[1] The service provider may become insolvent or have other difficulty to continue provision of the services and support.

	such are properly maintained in compliance with PDPO requirements. Legal advice should also be sought where necessary.
Guideline 3.4.5	*Access to data by the relevant authorities' examiners and the licensee's internal and external auditors should not be impeded by outsourcing. A licensee should ensure that adequate and effective arrangements are in place to facilitate the on-site examinations or off-site reviews, both announced and unannounced by authorized third parties (e.g. licensee's internal auditors, external auditors/assessors and the HKMA).*
Additional guidance	(a) Typically, an adequate arrangement includes a clause in the outsourcing agreements with service providers which allows for supervisory inspection or review of the operations and controls of the service provider (including unrestricted access by the relevant authorities, including the HKMA, to the relevant premises, systems, records and documents) as they relate to the outsourced activity, and that necessary prescribed consent to the arrangements should be obtained from the local authorities, if any, in the relevant jurisdictions.

4. General Risk Management and Internal Control Systems

Guideline section 4.2 – Risk management

Guideline 4.2.1		*A licensee should have in place effective risk management framework that is commensurate with the nature, scale and complexity of their operations to help ensure proper identification, monitoring and management of various risks. The risk management framework should be approved by the Board. A licensee should demonstrate that it has dedicated staff resources with sufficient professional knowledge, experience, and independence to oversee the quality of its risk management and internal control processes.*
Additional guidance	(a)	In case of introducing any initiative that may lead to material change on the risk profile of licensee, the licensee should critically review and assess the adequacy and effectiveness of its existing risk management framework and systems of control to ensure that they are adequate in identifying, monitoring and controlling the risks involved. The licensee should also step up its risk monitoring measures as appropriate, such as performing comprehensive reviews within a reasonable period after launch of the initiative, to ensure that no risks remain unidentified or unaddressed.

5. Information and Accounting Systems

Additional guidance will be provided as and when necessary.

6. Management of Float and SVF Deposit

Guideline section 6.2 - General principle

Guideline 6.2.1	*A licensee should have in place an effective and robust system to protect and manage the float and SVF deposit to ensure that all funds are deployed for prescribed usage only, that funds belonging to SVF users are protected against claims by other creditors of SVF issuers in all circumstances, and that funds are protected from operational and other relevant risks.*
Additional guidance	(a) Subsequent sections in this Chapter provide guidance on what constitute an effective and robust system. Some of the expectations are in respect of ensuring legal certainty and operational safety of float and SVF deposit. Typically, a licensee is expected to seek external legal opinion to ensure legal certainties and to commission external independent review to ensure operational soundness, and it is also expected that similar exercises be carried out before a licensee implement any significant changes to the system for protection and management of float and SVF deposit. A risk-based approach will be adopted such that if a licensee can provide sufficient justifications, other forms of independent verification may be considered. (b) The system for the protection and management of float and SVF deposit should be subject to independent review or audit at least on an annual basis to ensure its effectiveness and robustness. (c) A licensee should consult the HKMA before implementing any significant changes to the system for the protection and management of float and SVF deposit.

Guideline section 6.3 - Protection of float and SVF deposit

Guideline 6.3.1	*A licensee should put in place an effective trust arrangement to ensure the legal right and priority claim of the float and SVF deposit by users in the event of insolvency of a licensee. If justifications are provided*

	by a licensee, an effective bank guarantee and/or insurance coverage may be used as an alternative or supplementary arrangement. For the avoidance of doubt, money in transit arising from an SVF user choosing direct debit from his/her bank account or credit card account instead of his/her SVF user account are treated as float received from the SVF user and should accordingly be accorded the same level of protection.
Additional guidance	(a) Among other effective trust arrangements, a trust arrangement in which a licensee makes a declaration of trust of holding the assets of the float and SVF deposit in the segregated accounts with licensed banks or a foreign bank recognized by the HKMA is acceptable. A licensee should properly designate such segregated bank accounts for holding float and SVF deposit under its trust arrangements. For instance, relevant details of the designated bank account(s) should be included (i) in the declaration of trust; (ii) as an annex to the relevant declaration of trust; or (iii) in a register maintained in accordance with the arrangements and procedures set out in the declaration of trust. The process for bank account designation should also be approved by an appropriate authority (e.g. the Board of Directors or Chief Executive) with audit trail. (b) All monies payable to (e.g. account top-up) or receivable from an account (e.g. payments to merchant) within an SVF scheme, including money in transit, should be treated as float and be accorded with the same level of protection. Monies payable into merchants' SVF accounts, regardless of whether such monies originate from another SVF user account or direct debit from his/her bank account or other card account, should also be treated as float and be accorded with the same level of protection..
Guideline 6.3.2	*Where circumstances warrant a trigger to refund the float and SVF deposit to users, the trust arrangement should operate to the effect that proper legal positions and authorisations are in place to ensure a smooth and efficient refund process.*

Additional guidance

Under the trust arrangement, a licensee should have, among other things, in place exit plan which, typically with board level endorsement, should include the following:

(a) A list of specific circumstances that would trigger a mechanism to refund the float and SVF deposit to users (e.g. a decision to exit the SVF business, liquidation). Where applicable, monitoring indicators should be developed to ensure timely trigger of exit plan upon materialisation of the specified circumstances.

(b) Detailed procedures to ensure a smooth and efficient refund process. In assessing the efficiency of the refund process, the HKMA will consider factors including but not limited to notification to relevant users, the duration in which a user is expected to receive the refund, the steps that a user need to take to seek for refund, and the extent of possible refund failure (e.g. unable to contact users).

(c) An assessment of the legal certainty and operational feasibility of the procedures.

Guideline 6.3.3	*A licensee should ensure that there are sufficient funds for the refund of the float and SVF deposit to all SVF users at all times and there are sufficient additional funds to pay for the costs of distributing the float and SVF deposit to all SVF users in case of need.*

Additional guidance

(a) A licensee is expected to perform a regular and prudent estimation of the cost required to effectively perform the refund process having regard to factors such as the amount of users and float and SVF deposit (including any money-in-transit which should be refunded to users in the event of exit) as specified in its exit plan (see 6.3.2). Based on such cost estimation, a licensee should establish effective process to ensure sufficient additional funds are at all times available and reserved for processing the refund. For example, such funds can be maintained in the form of surplus/buffer to the float and SVF deposit. A licensee should have in place adequate policies and procedures on how such surplus/buffer should be determined,

e.g. the relevant factors and formulas (if applicable). Adequate controls should also be in place to document the determination and maintenance of such surplus/buffer, and for monitoring the effectiveness and robustness of the related arrangements.

(b) Where the amount of funds in the relevant account(s) for holding the assets of the float and SVF deposit is less than the amount of float and SVF deposit as recorded in the ledger system, i.e. a shortfall exists, a licensee should escalate the case to its senior management and the HKMA promptly and with no undue delay. In general, the report to the HKMA should cover, among others, the cause and relevant details of the case, and the actions taken to rectify the shortfall.

Guideline 6.3.5	*The assets, including cash and bank deposits, in which the float and SVF deposit of an SVF scheme are held should be segregated from the licensee's own funds as well as funds received for the licensee's other business activities.*
Additional guidance	(a) Where a licensee operates more than one SVF scheme, it is generally expected that the float and SVF deposit of each of the SVF schemes are held in a segregated manner.
Guideline 6.3.6	*A licensee should put in place effective internal control measures and procedures, which constitute an integral part of the licensee's overall robust internal control system, to protect the float and SVF deposit from all operational risks, including the risk of theft, fraud and misappropriation.*
Additional guidance	(a) To ensure effectiveness of a control system for protecting the float and SVF deposit, a licensee would normally need to put in place a tailor-made system of controls, typically with board level endorsement, that fits the risk characteristics of its business model, operational processes, and system design. The controls set out below serve to illustrate certain commonly established internal control measures: (i) Segregation of duties**:** Front line business, back office operations and control functions should be independent of each other and appropriately segregated to ensure

sufficient checks and balances. A clear reporting line should be established for each of the functions, which should normally be headed by senior management staff of similar seniority in order to ensure independence;

(ii) Control policies and procedures (P&P): P&P should be unambiguous, actionable with clear criteria, triggers and/or indicators. They should be regularly reviewed taking into account, among other things, any changes to the business model, scale of business operations, operational processes, technology applications, stakeholders' feedback as well as rules and regulations.

(iii) Risk identification and mitigation: A licensee should undergo a rigorous process to identify all possible risks and vulnerabilities that may give rise to, among other things, fraud, theft, misappropriation or any other forms of operational losses. A licensee is expected to include in its P&P specific control steps that can effectively address the identified risks and vulnerabilities

(iv) Authorization controls: A general expectation for an effective control system is the presence of (a) stringent authorization procedures to ensure all key operations are properly authorized, e.g. operation of bank accounts, changes to the list of authorized merchants; (b) timely detection and prevention of unauthorized activities; (c) diligent follow up or investigation of incidents suggesting attempts to perform unauthorized activities.

(v) Internal control procedures: While detailed internal control procedures could vary significantly among licensees, typical internal control methods, including maker-checker arrangement and regular reconciliation of accounts, should be established in all key business and operation processes as well as all important system input or updating procedures. A licensee should ensure that the personnel responsible for monitoring any triggering

event are familiar with the relevant operations. A licensee should also have in place adequate systems of control to ensure that any external parties (e.g. custodian) that is responsible for carrying out certain functions (e.g. reporting functions) fully understand their responsibilities.

(b) Without in any way constraining licensees from applying more advanced and effective controls, below sets out the key control components expected of in a typical mode of operations:

(i) A well tested and strictly implemented process to ensure timely and accurate records of funds paid into and out of a licensee's float and SVF deposit, with regular reconciliation between system records and the actual float and SVF deposit (e.g. balances of the dedicated bank account holding float and SVF deposit). Regular MIS should be made available in a timely manner at regular intervals during a day. Arrangement should be made to enable the HKMA to have effective access to the MIS with a view to performing random offsite supervisory checking. Exceptions identified during reconciliation are expected to be escalated internally and investigated in a timely manner. Significant exceptions (to be agreed between the HKMA and a licensee) should be reported to the HKMA as soon as they are identified.

(ii) A well tested and strictly implemented process to enable effective screening of payment transactions to ensure that payments are made to authorized payees only. It is expected that a licensee's system design can enable early detection of payment instructions to non-approved payees such that these instructions will be put on hold and subject to additional review.

(iii) Additional measures that provide further protection to the safety and sufficiency of float and SVF deposit. Possible forms of additional protection include effective

payment controls by an independent third party (e.g. a licensed bank or a foreign bank recognized by the HKMA), insurance coverage, or guarantee by a bank or other creditworthy parties such as a financially strong group company. For the avoidance of doubt, these are options only and a licensee can propose for the HKMA consideration other effective means of providing further protection. The extent to which additional protection is required will depend on a host of factors, including among other things the HKMA's assessment of the effectiveness and robustness of a licensee's internal controls on float protection, the size and fluctuation of float and SVF deposit, and the financial strength of the licensee. The licensee shall discuss and agree with the HKMA on the detailed arrangement during its ongoing supervisory process.

Guideline section 6.4 - Management of float and SVF deposit

Guideline 6.4.1	*Float and SVF deposit of an SVF scheme should be managed mainly for the purpose of liquidity management to ensure that there will always be sufficient funds for redemption. A licensee should put in place effective liquidity management policies, guidelines and control measures commensurate with the mode of operation of the SVF scheme in respect of the assets in which the float and SVF deposit are held.*
Additional guidance	(a) Among other scenarios, a licensee will be subject to higher liquidity requirements when a user is able to utilise or withdraw the relevant funds of his/her SVF account immediately after an account top-up, albeit the relevant funds associated with the account top-up will not be paid into the licensee's designated bank account(s) for holding float some time later (which could be several business days). Such liquidity requirements may change rapidly and dynamically due to a different external factors such as any campaigns that may incentivise a user to use a particular top-up channel and/or a particular SVF service/function. A licensee should have in place effective mechanisms to monitor and estimate its liquidity requirements, and

take timely and sound measures to manage and address its liquidity requirements.

(b) In assessing the effectiveness of the control measures, the HKMA takes into account, among others, the licensee's expertise and track records in managing its liquidity requirements.

Guideline 6.4.2	*A licensee should not adopt a business model that takes investment returns from float management as a significant source of income. A licensee proposes to hold a proportion of the float and SVF deposit in low risk financial assets other than cash or bank deposits should obtain the HKMA's prior written consent by demonstrating to the HKMA that the float and SVF deposit will be adequately protected from all relevant risks, including investment risk, market risk, concentration risk and liquidity risk, etc. The licensee seeking the HKMA's prior consent should at least put in place adequate investment policies and guidelines and effective control measures to protect the float and SVF deposit from all relevant risks.*
Additional guidance	(a) In assessing the effectiveness of the control measures, the HKMA takes into account, among others, the licensee's expertise and track records in managing the investments.
Guideline 6.4.3	*Unless effective currency risk management policies, guidelines and control measures are put in place, mismatch between the currency denomination of the float or SVF deposit and that of the assets in which the float and SVF deposit are held is generally not allowed except for the mismatch between HK dollar and US dollar positions.*

Additional guidance	(a)	If there are legitimate reasons that render it inevitable for a licensee to run a currency mismatch between the float and SVF deposit and the assets in which such float and SVF deposit are held, a licensee can approach the HKMA to explain the situation. Should the HKMA accept the need for such a currency mismatch, the licensee will be expected to put in place appropriate policies and procedures to monitor or manage the foreign exchange risk arising therefrom and to ensure the sufficiency of float and SVF deposit.

7. Specific Risk Management

Guideline section 7.2 - Technology risk management

Guideline 7.2.1	*A licensee should establish an effective technology risk management framework to ensure (i) the adequacy of IT controls, (ii) the quality and security, including the reliability, robustness, stability and availability, of its computer systems, and (iii) the safety and efficiency of the operations of the SVF. The framework should be "fit for purpose", i.e. commensurate with the risks associated with the nature, size, complexity and types of business and operations, the technologies adopted and the overall risk management systems of the licensee. A licensee should allocate its technology resources between business development and risk management appropriately to ensure that sufficient resources are devoted to the latter.*
Additional guidance	In assessing the effectiveness of a licensee's Technology Risk Management (TRM) framework, the HKMA will take into account the following general expectations: (a) An effective TRM framework normally comprises proper IT governance, a continuous technology risk management process and implementation of sound IT control practices: **IT governance** (b) Typically, IT governance covers various aspects, including a clear structure of IT functions and the establishment of IT control policies. (c) While there could be different constructs, a typical TRM framework comprises at least three major functions: (i) IT function responsible for delivering day-to-day technology services and support to business units. (ii) TRM function responsible for ensuring that the licensee follows a robust TRM process (see further details at paragraph (e) and (f) below and applies technology to

effectively manage other risks, in particular operational risk.

(iii) IT audit function responsible for ensure sufficient audit coverage of a licensee's IT controls and TRM process and that all deficiencies are promptly escalated, followed-up and rectified.

(d) While a licensee should establish a set of IT control policies that fits its business model and technology applications, set out below are some generally expected features:

(i) A set of IT control policies which establishes the ground rules for IT controls is developed. These policies are formally approved and properly implemented among IT functions and business units.

(ii) Processes used to verify compliance with IT control policies and the process for seeking appropriate approval for dispensation from IT control policies are specified clearly, and consequences associated with any failure to adhere to these processes are in place.

(iii) The roles and responsibilities of IT functions, TRM function and IT audit function as well as the responsibilities of senior management to oversee the performance of IT functions are clearly specified.

(iv) Clear processes are in place to regularly review the sufficiency and competence (in terms of professional expertise, relevant experience and familiarity with the licensee's operations) of staff holding the responsibilities mentioned in sub-paragraph (iii) above.

Technology risk management process

(e) A licensee should put in place an effective risk management system that fits its specific business model and risk profile. The sophistication of the risk management system should be commensurate with the scale and complexity of a licensee's

business.

(f) Among other things, a robust process should be established to manage all changes (e.g. changes arising from new products, services, processes, contract terms, or any changes of external factors such as law and regulations) that might change a licensee's technology risk exposures. Such a process should be able to capture all proposed changes, subject them to rigorous risk identification process. All identified risks should be critically evaluated, monitored and controlled on an on-going basis.

Implementation of sound practices in respect of IT controls

(g) A licensee should implement adequate sound practices in respect of IT controls that fit its business model and risk profile. In assessing the adequacy of IT controls, the HKMA will consider the good practices on various areas set out in Annex.

Guideline 7.2.2	*Given that the risk of IT operational incidents (e.g. service interruptions) cannot be completely eliminated, a licensee should establish an incident management framework with sufficient management oversight to ensure effective incident response and management capability to deal with significant incidents properly. This includes (i) timely reporting to the HKMA of any confirmed IT-related fraud cases or major security breaches, including cyber attacks, cases of prolonged disruption of service, and systemic incidents where users suffer from monetary loss or frustrating user experience (e.g. data leakage) and (ii) a communication strategy to address the concerns of any stakeholders may have arising from the incidents and restore the reputational damage that the incidents may cause.*
Additional guidance	(a) To ensure sufficient management oversight and capability of an incident management framework, a licensee should assign clear duties, with appropriate authorities, to individual management staff responsible for handling different risks (e.g. IT risk, operational risk, legal/regulatory risk and reputational risk) that might stem from any significant incident. Such staff should have sufficient seniority. A licensee is expected to define clearly in writing the types of incidents that would be considered significant,

taking into account their scale and nature of business (see paragraph (c) below). Robust arrangement should be put in place to ensure that all responsible management staff would be timely alerted of any significant incident. They are expected to communicate proactively with one another to evaluate the situations and identify the most appropriate course of actions in order to manage all relevant risks effectively.

(b) Among other things, a licensee should strive to restore normal IT service as quickly as possible with the least impact to the licensee's business operations. To this end, a licensee should have in place effective incident response and management procedures which, as a minimum, should allow the licensee to:

(i) find out quickly the possible root cause of the incident (such as whether it arises from weaknesses in the licensee's security controls or operating environment) and assess the potential scale and impact of the incident (e.g. whether the incident is likely to affect other users or even the users of other external parties);

(ii) contain, as soon as practicable, the damage to the licensee's user assets, data and reputation, and resolve the incident where the resolution timeframe is commensurate with the severity level of the incident. The top priority should be to protect the interests of users who have been or may be affected by the incident;

(iii) escalate the incident promptly to the senior management especially if the incident may result in reputation damage or material financial loss;

(iv) notify promptly the affected users and other affected external parties (so that they can in turn notify their affected users) where appropriate;

(v) collect and preserve forensic evidence as appropriate to facilitate subsequent investigation and prosecution of

offenders if necessary;

(vi) regularly report the progress of the incident resolution; and

(vii) perform a post-mortem review of the incident, covering the identification of the root cause and the generation of action plans for rectification actions needed (e.g. preventive and detective controls, mitigating controls).

(c) Under a typical incident management framework, an appropriate severity level is required to be assigned to each identified incident to enable a timely response to significant incidents. Among other things, criteria used for assessing severity levels of incidents shall be established and documented. Sufficient training shall also be provided to relevant staff such that they can effectively discern incidents of high severity level.

(d) Under a typical incident management framework, an incident response team, which should comprise team members from relevant functions, is established to support the senior management staff in managing and responding to incidents in accordance with established procedures. The roles and responsibilities of the team, which includes recording, analysing, remediating and monitoring incidents, are clearly defined and documented.

Guideline 7.2.3	*A licensee should have in place adequate measures to maintain appropriate segregation of databases for different purposes to prevent unauthorized or unintended access or retrieval and that robust access controls are enforced to ensure the confidentiality and integrity of the databases. In respect of any personal data of users, including merchants, a licensee should at all times comply with the PDPO as well as any relevant codes of practice, guidelines or best practice issued by the Office of the PCPD from time to time.*
Additional guidance	(a) A licensee should follow relevant best practices issued by the PCPD. Examples include the PCPD's recommendations on best

practices with respect to online tracking and use of cookies on websites including Internet websites and mobile apps.

(b) In a typical setting, a licensee should implement, among others, the following controls to protect the confidentiality and integrity of databases:

(i) Access to the information and application systems is restricted by an adequate authentication mechanism associated with access control rules. A role-based access control framework is adopted and access rights are only granted on a need-to-have basis.

(ii) A security administration function and a set of formal procedures are established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities.

(iii) Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) is implemented to mitigate the risk of unauthorized activities being performed by the security administration function.

(c) Due care should be exercised when controlling the use of and access to privileged and emergency identifications (IDs). In a typical case, the necessary control procedures include:

(i) changing the default password;

(ii) restricting the number of privileged users;

(iii) implementing strong controls over remote access by privileged users;

(iv) granting of authorities that are strictly necessary to privileged and emergency IDs;

(v) formal approval by appropriately senior personnel prior to

being released for usage;

(vi) logging, preserving and monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);

(vii) prohibiting sharing of privileged accounts;

(viii) proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data centre); and

(ix) changing of privileged and emergency IDs' passwords immediately upon return by the requesters.

Guideline section 7.3 - Payment security management	
Guideline 7.3.2	*A licensee should have adequate policies and procedures on the ownership, classification, storage, transmission, processing and retention of information collected from users through registration of SVF service and execution of payment transactions to ensure confidentiality and integrity of the information.*
Additional guidance	In assessing the adequacy of policies and procedures on payment security management, the HKMA will consider the following from both IT's and not-IT's perspectives: (a) Information ownership For information being collected, processed, created, maintained by a licensee, the licensee should assign a dedicated person as information owner. The information owner is generally accountable for classification, usage authorization and protection of information processed by and stored in systems. (b) Information classification Information should be classified into different categories according to the degree of sensitivity to indicate the extent of

protection required. To aid the classification process, a licensee should develop guidelines and definitions for each classification and define an appropriate set of procedures for information protection in accordance with the classification scheme.

(c) Information in storage

Sensitive data stored in end-user devices as well as the backend systems of SVF licensees, such as payment data, personal identifiable information (PII) and authentication data should be appropriately secured against theft and unauthorized access or modification. They should be encrypted and stored in a secure storage environment, using strong and widely recognised encryption techniques. In addition, proper testing cases should be included during the formal acceptance process to ensure that all relevant controls to protect such data (e.g. controls against electronic pick-pocketing) are covered.

(d) Information in transmission

A licensee should ensure that when transmitting sensitive data, e.g. from a user's device to a licensee's server, a strong and secure end-to-end encryption is adopted and maintained in order to safeguard the confidentiality and integrity of the data, using strong and widely recognised cryptographic techniques.

Where applicable, communication channels for data exchange should only be open on a need-to-use basis. For example, where it is practical to do so, communications via contactless channels should only be allowed after activation by the user and within a limited time window.

(e) Information in processing

If a licensee offers merchant acquiring services, it should require its merchants to have necessary measures in place to protect sensitive data related to payments, and should refrain from providing services to merchants which cannot ensure such protection. The licensee should also implement sufficient

controls to maintain and verify the integrity of the information processed by its systems.

(f) Information retention and disposal

A licensee should implement an information retention and disposal policy to limit the data storage amount and retention time, having regard to applicable legal, regulatory, and business requirements. Processes should be in place for secure deletion of data that is no longer needed.

(g) Information minimisation

In designing, developing and maintaining payment services, a licensee should ensure that information minimisation is an essential principle of the core functionality: gathering, routing, processing, storing and/or archiving, and visualisation of sensitive data should be kept at the absolute minimum level. Unnecessary information should not be present in systems and processes that do not require it. For example, user account information which may be held by a licensee in its backend systems (e.g. cardholder names) should not be stored or accessible on user-controlled frontend devices or applications that do not require such information to complete transactions. Also, data used by a licensee's payment applications should not be accessible by other applications stored on users' devices (i.e. "application sandboxing" or "application containerisation").

Guideline 7.3.3	*A licensee should implement adequate security measures to protect each payment channel (including cards and user devices) provided to users for using its SVF against all material vulnerabilities and attacks.*
Additional guidance	In assessing the adequacy of security measures for payment channels, the HKMA will consider the following:

(a) Payment card

A licensee providing payment card services should implement adequate safeguards to protect sensitive payment card data. A typical example is the deployment of chip cards to store those

data and the implementation of strong card authentication methods for point-of-sale and ATM card transactions. Under a risk-based approach, for cards of which have higher limits and functions (e.g. those in which customer identity has been verified):

(i) a physical card should be embedded with chip unless the card bears the same features as an unverified card (or gift card);

(ii) chip-based authentication should be enforced if a physical card can be used for local ATM transactions; and

(iii) effective risk mitigating measures (e.g. lower transaction limits, notification arrangement, fraud monitoring and providing customers with a feature to activate/deactivate relevant feature with the flexibility to set a lower withdrawal limit) should be implemented if a physical card can be used for overseas ATM cash withdrawal.

(b) User device

A licensee should assume that user devices are exposed to security vulnerabilities and take appropriate measures when designing, developing and maintaining payment services. Security measures should be in place to guard against different situations, including unauthorized device access, malware or virus attack, compromised or unsecure status of mobile device and unauthorized mobile applications.

(c) Mobile device for payment acceptance

If mobile devices are used by merchants to accept a licensee's payment solutions, additional security measures should be implemented to safeguard the mobile payment acceptance solution, including the detection of abnormal activities and logging them in reports, and the provision of merchant identification for users to validate its identity.

(d) Contactless payments[2]

To guard against potential malicious attacks and to address the risk of data leakage, loss or theft of user's device/card, a licensee should implement adequate and effective security controls for contactless payment which include, among others, the following:

(aa) sensitive data required for making contactless payments should be stored and accessed securely;

(ab) unnecessary data should not be stored in a way that can be easily captured by unauthorised parties;

(ac) additional controls should be implemented (e.g. additional factor of authentication, short validity period of dynamic payment credential or lower payment limit) if payment credential is subject to relay attack; and

(ad) static payment credential that can be used for making contactless payment at POS should be prohibited from conducting non-POS transactions unless such payment credential is not subject to the risk of being captured by unauthorised parties during the contactless transaction.

Adequate and effective security controls should be implemented to prevent and detect unconfirmed/incomplete transactions (e.g. due to interference or other operational reasons) and facilitate a timely refund to customers.

Guideline 7.3.4	*A licensee should implement adequate payment security controls to ensure the authenticity and traceability of payment transactions and detect fraudulent transactions.*
Additional guidance	In assessing the adequacy of security controls set out in Guideline 7.3.4, the HKMA will consider the following: (a) User authentication

[2] Contactless payment refers to the use of contactless or wireless technology (e.g. QR Code and Near Field Communication (NFC) technology) to transmit payment credential (e.g. payment card information) between the customer's device (e.g. physical card, mobile device) and the payee (e.g. a merchant).

(i) In considering using single authentication factor or combination of authentication factors, a licensee should take into account the risk of the operation(s) that can be done after the authentication is passed and observe, among others, the following requirements:

(aa) consider the maturity and effectiveness of authentication factor or combination of authentication factors both before adoption and on a regular basis thereafter;

(ab) implement effective controls in enrolment, change and withdrawal of authentication factor to ensure that it is properly initiated by the *bona fide* user;

(ac) if digital certificate is used as an authentication factor, ensure that the digital certificate and its associated key are non-duplicable and stored in a secured manner, where applicable; and

(ad) for e-wallets, as the effectiveness of authentication will likely be weakened if authentication factor is derived from, can be found or accessible from the same mobile device where the e-wallet is installed (e.g. users are allowed to use the same mobile device to access e-wallets and receive SMS OTP or generate OTP as an authentication factor), a licensee should consider effective controls that are commensurate with the risk profile under various scenarios. Examples include requiring an additional factor of authentication which is independent from the mobile device and/or implementing other effective controls (e.g. enhanced fraud monitoring, lower storage/transaction limits and limiting functions/features).

(ii) A licensee should select reliable and effective authentication techniques to validate the identity and authority of its users. User authentication is stronger

when combining any two or more of the following three factors (i.e. two-factor authentication (2FA)):

(aa) something a user knows (e.g. user IDs and passwords);

(ab) something a user has or possesses (e.g. one-time passwords generated by a security token or a licensee's security systems); and

(ac) something a user is (e.g. retina, fingerprint or voice recognition).

(iii) If a password (including a personal identification number (PIN)) is used as one factor of authentication, a licensee should put in place adequate controls related to the strength of the password (e.g. minimum password length).

(iv) Where an OTP is used as an authentication factor, a licensee should observe, among others, the following requirements where applicable:

(aa) implement sound key management practices to safeguard secret code (e.g. seed values) for generating OTP;

(ab) conduct regular assessment on the adequacy and effectiveness of OTP;

(ac) include sufficient information for user to identify the purpose of OTP and relevant transaction;

(ad) conduct appropriate and effective authentication before allowing a user to change mobile number or device for receiving OTP; and

(ae) if SMS OTP is used, make necessary arrangements so that deliver of the SMS OTP is to the registered mobile number only even if SMS forwarding service is enabled.

(b) Login attempts and session management

(i) Effective controls include limiting the number of login or authentication attempts (e.g. wrong password entries), implementing time-out controls and setting time limits for the validity of authentication. If one-time password (OTP) is used for authentication purpose, a licensee should ensure that the validity period of such passwords is limited to the strict minimum necessary.

(ii) If the maximum number of failed login or authentication attempts is implemented and is reached, access to the payment service should be temporarily or permanently blocked. Inactive payment service sessions should also be automatically terminated after a pre-defined maximum duration.

(c) Activities logging

(i) A licensee should have processes in place ensuring that all transactions are logged with an appropriate audit trail. Its service should incorporate security mechanisms for the detailed logging of transaction data, including the transaction ID, time stamp, parameterisation change as well as access to transaction data.

(ii) A licensee should have robust log files allowing retrieval of historical data including a full audit trail of additions, modifications or deletions of transactions. Access to such tools, including privileged responsibilities, should only be available to authorized personnel and should be appropriately logged.

(iii) Where payments can be initiated via different channels, the payment channel should be clearly identifiable in the log files. A licensee should also identify and keep track of the source through which the payment was initiated (e.g. point-of-sale, Internet) and the recipient of the payment.

(iv) Channels should be provided for users to check their past transactions. If there is a fee for the use of a channel, the fee should be of a reasonable amount and users are notified.

(d) Fraud detection systems

(i) A licensee should operate transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions. Suspicious or high-risk transactions should be subject to a specific screening, filtration and evaluation procedure.

(ii) Where an SVF enables a user to bind a credit/debit/prepaid card as a funding source for his/her SVF account, the licensee should implement appropriate verification arrangements, to be conducted by the card issuer with the cardholder (e.g. SMS OTP or other effective measures), to confirm that cardholder gives consent to the card binding. Such verification arrangement should be triggered at least during the binding process or when the card is initially used by the relevant SVF account. Licensees should disallow binding a card if the relevant card issuer does not support the verification arrangement required by the licensee or fails to perform the required verification with the relevant cardholder.

(iii) Where an SVF enables a user to set up a direct debit from a bank account, the licensee should implement appropriate measures to ensure that the setting up of such a direct debit has been authorised by the relevant bank account owner. In this regard, licensees shall refer to relevant measures promulgated by the HKMA on 26 October 2018 as well as other guidance as appropriate.

(iv) Where a licensee, according to its risk policies, decides to block a payment transaction which has been identified as potentially fraudulent, the licensee should maintain the duration of the block as short as possible until the security issues have been resolved. A licensee's monitoring staff

should be promptly alerted by their monitoring mechanism if suspicious online transfers and unusual activities are initiated. In these cases, the licensee should, as soon as practicable, check with the users of these transactions or activities.

(v) A licensee should implement effective measures to guard against automated brute-force attacks and credential stuffing using automated tools during customer account login.

(e) Account maintenance

(i) A licensee should implement appropriate security controls and authentication for high risk account maintenance functions such as change of password, password reset, request or change of registered device and change of mobile number for receiving SMS OTP, change of verified account owner, increase of transaction limit, etc. As a good practice, a licensee should remind users whose passwords remain unchanged for a prolonged period to change their passwords regularly.

(ii) A licensee should implement additional controls for an account with which no transaction has been conducted for a prolonged period (idle account). For instance, a licensee may deactivate payment function of an idle account until it is satisfied that it continues to be used by the *bona fide* user.

(f) Account Aggregation Service

(i) To properly manage relevant risks (e.g. legal, reputation and operation risks) that may arise from the provision of Account Aggregation Service (AAS)[3] through partnership with other institutions, a licensee should implement effective controls before launching the service. These

[3] Where a licensee offers AAS, it generally allows its users to access their accounts maintained in other institutions (which could be in overseas institutions) through e-wallet or platform operated by the licensee without requiring the users to separately log in to the platform of those institutions.

include, but not limited to, the following:

(aa) conduct independent legal due diligence;

(ab) implement appropriate controls for customer protection such as handling of customer complaints and apportionment of liability for any financial loss of customers that may arise;

(ac) ensure compliance with applicable local or overseas legal and regulatory requirements, including personal data privacy requirements where applicable;

(ad) assess and eliminate the risk of intrusion to licensees' systems and networks through any connections with the partnering institutions; and

(ae) make proper disclosure to customers about the risks and limitations of AAS.

Guideline 7.3.5	*A licensee should authenticate the identity of SVF users before they can administer their SVF accounts and initiate high-risk transactions. Timely notification should be sent to users after these activities.*
Additional guidance	In assessing a licensee's compliance with Guideline 7.3.5, the HKMA will consider the following (a) Administration of user accounts (i) If a licensee allows a user to open an account through online channel, a reliable method should be adopted to authenticate the identity of the user. (ii) A licensee should perform adequate identity checks when any user requests a change to the user's account information or contact details that are useful for the user to receive important information or monitor the activities of the user's accounts. In addition, the licensee should take

measures to prevent and detect possible frauds related to these changes.

(b) Controls over high-risk transactions

(i) A licensee should take into account relevant factors such as their risk profile and assessment, as well as the effectiveness of authentication methods in determining the types of transactions that are considered high-risk. A licensee should implement effective controls, such as 2FA or other risk mitigating measures, commensurate with such risk where circumstances permit to re-authenticate the user before effecting each high-risk transaction. High-risk transactions should, at least, include:

(aa) transactions that exceeded the predefined transaction limit(s);

(ab) change of personal contact details which may enable users to monitor the account activities;

(ac) unless it is not practicable to implement in the SVF concerned, transactions that exceeded the aggregate rolling limit(s) (i.e. total value of transactions over a period of time);

(ad) binding social media account for the purpose of receiving OTP or notification, etc.;

(ae) activation of payment without PIN function (applicable to merchant payment only)[4]; and

(af) display of full contact details of a user on e-wallet or QR code.

(ii) A licensee should define the per transaction limit(s) and,

[4] In this case, licensees should also clearly make known to customers that they have activated such function. This requirement also applies if this function is activated by default at the time of account opening. For the purpose of this requirement, payment without PIN function should generally not be made available to P2P transactions.

unless it is not practicable to implement in the SVF concerned, the aggregate rolling limit(s), having regard to factors such as its fraud monitoring capability, maximum stored value per SVF (if applicable), maximum daily top up limit (if applicable) and other fraud protection mechanism implemented. Such limits should be clearly communicated to users.

(c) Notifications to users

(i) To facilitate timely detection of unauthorized transactions that may arise as a result of fraudulent activities, a licensee should, as far as practicable, notify users immediately via an effective channel once the users initiate high-risk transactions or transactions exceeding user-defined thresholds made on their accounts, if applicable. The transaction alert should include information such as source and amount of the transaction to assist users in identifying a genuine transaction.

(ii) A licensee should take into account its risk profile and assessment in determining the types of transactions that should be followed by sending a notification to users via an effective channel. As a general benchmark, the following types of transactions should send out a notification:

(aa) transaction that are not conducted at POS (e.g. card-not-present transactions);

(ab) high-risk QR code payments;

(ac) high-risk overseas card POS transactions;

(ad) high-risk ATM cash withdrawal;

(ae) suspicious account login or account login without 2FA;

(af) change of payment limit;

(ag) activation of payment without PIN;

(ah) change of contact information;

(ai) change of authentication method;

(aj) making payment without PIN (non-device based only); and

(ak) fund transfer to third party without 2FA (non-device based only).

(iii) In determining the choice of notification channel (e.g. SMS, email or in-app notification), a licensee should have regard to the risk of transaction and the effectiveness of such channel. Where SMS notification is used, licensees should implement relevant controls with mobile network operators to ensure that such SMS notification is delivered to both pre-registered mobile number and forwarded Hong Kong mobile number (if the user has enabled SMS forwarding service for his/her mobile number).

(iv) Where user requests licensees to opt out from such notifications, a licensee should ensure that proper due processes and procedures are in place to, among others:

(aa) explain to the user the potential risks and any other service implications if no notification is sent to the user, and request the user to confirm his or her understanding of the risks and implications;

(ab) properly authenticate the user to ensure that the request is from the *bona fide* user (where applicable);

(ac) allow the user to opt in if requested; and

(ad) maintain proper records related to the above process.

Guideline 7.3.6	*A licensee should provide advice and assistance to users on the secure use of SVF through an effective communication channel.*
Additional guidance	In assessing a licensee's compliance with Guideline 7.3.6, the HKMA will consider the following: (a) Security advice for users (i) A licensee should warn its users of the obligations to take reasonable security precautions to protect their devices used in payment and keep their passwords used for accessing payment service secure and secret. Moreover, the licensee should provide easy-to-understand, prominent and regularly reviewed advice from time to time via effective methods and multiple channels to its users on security precautionary measures. (ii) In addition, a licensee should manage the risk associated with fraudulent emails, websites, messages, social media, and mobile Apps and the like which are designed to trick its users into revealing sensitive user information such as personal data (e.g. name and identification number) and credentials (e.g. login IDs, passwords and OTP). In particular, the licensee should search the Internet and App stores regularly for fake or suspicious websites, messages, social media or Apps. Whenever a licensee is aware of fake or suspicious emails, websites or Apps that might give the public a false impression that they originated from the licensee or that its Apps can be downloaded from unofficial sources, the licensee should make a timely decision on whether there is a need to inform its users and the public, and report the matter to the Police and the HKMA. For avoidance of doubt, where frauds involve phishing websites or messages that are designed to trick users of a licensee and/or the public into revealing sensitive user information such as personal data and credentials, the licensee should, as part of its handling, alert its users and the public by issuing a press release and report the matter to the Police,

the HKMA, as well as other relevant regulator(s), if any. The press release as well as the relevant information such as but not limited to the hyperlinks of the phishing websites, if applicable, should be shared with the HKMA in a timely manner.

(b) Communication with users

(i) A licensee should provide at least one secure channel for ongoing communication with users regarding the correct and secure use of the payment service. A licensee should inform users about this channel and explain that any message on behalf of the licensee via any other means is not reliable. Through the secure channel, a licensee should keep users informed about updates to security procedures regarding payment services. Any alerts about significant emerging risks should also be provided via the secure channel. The relevant channels should be effective taking into account the mode of delivery and usual communication channels of the licensee's product.

(ii) To manage the risks arising from different forms or modes of scamming activities, a licensee should not send, generate or trigger any message (e.g. emails, SMS messages, or similar kinds of instant messages) to the users with embedded hyperlinks that would (a) request users to provide sensitive user information such as personal data and credentials; or (b) direct a user to its website or Apps for transactions. A licensee should stand ready to remind users that they would not conduct the foregoing where considered necessary.

(iii) User assistance should be made available by a licensee for all questions, complaints, requests for support and notifications of anomalies or incidents regarding payments and related services, and users should be appropriately informed about how such assistance can be obtained with regard to a possible involvement of third parties.

Guideline 7.3.7	*A licensee should guard against current and upcoming cyber security risks associated with its SVF by monitoring the trends in cyber threats, implementing adequate protective measures and performing periodic security testing.*
Additional guidance	In assessing a licensee's compliance with Guideline 7.3.7, the HKMA will consider the following: (a) Cyber security risk management process Where a licensee is heavily reliant on Internet and mobile technologies to deliver its services, cyber security risks should be adequately managed through the licensee's TRM process. The licensee should also commit adequate resources to ensure its capabilities to identify the risk, protect its critical services against the attack, contain the impact of cyber security incidents and restore the services. (b) Cyber threat intelligence A licensee should keep pace with the trends in cyber threats. It may consider subscribing quality cyber threat intelligence services, which are relevant to its business, to enhance its ability to precisely respond to new type of threats in a timely manner. The licensee may also seek opportunities to collaborate with other organisations to share and gather cyber threat intelligence with the aim of facilitating the SVF industry to better prepare and manage cyber security risks. (c) Penetration testing A licensee should regularly assess the necessity to perform penetration testing. Coverage and scope of testing should be based on the cyber security risk profile, covering not only networks (both external and internal) and application systems but also social engineering and emerging cyber threats. It should also take appropriate actions to mitigate the issues, threats and vulnerabilities identified in penetration testing in a

timely manner, based on the impact and risk exposure analysis.

(d) Internet connected device

As Internet evolves, more devices or appliances are embedded with Internet connectivity. These devices with "always on" network connectivity may create more end points which allow intruders to get access to a licensee's critical IT infrastructure. The licensee should pay attention to related risks and take appropriate measures accordingly.

Guideline 7.3.8	*A licensee should provide efficient and reliable SVF payment services which are commensurate with the mode of operation of its SVF.*
Additional guidance	(a) In typical situations, efficiency and reliability should be assessed by measurable performance indicators such as response time, transaction throughput, system capacity, system availability and stability. A licensee should test and monitor the performance of its SVF against the predefined indicators to its efficiency and reliability. For SVF serving merchants where high performance is required (such as public transport operators), a licensee should agree with the merchants on the expected performance indicators and commit sufficient resources to ensure conformity.

Guideline section 7.4 - Business continuity management

Guideline 7.4.1	*A licensee should have in place adequate business continuity management (BCM) programs to ensure continuation, timely recovery, or in extreme situations orderly scale-down of critical operations in the event of major disruptions caused by different contingent scenarios.*
Additional guidance	(a) In typical situations, an adequate business continuity management program consists of business impact analysis, recovery strategies, a business continuity plan and alternative sites for business and IT recovery, which are elaborated in the ensuing paragraphs.

Business impact analysis

(b) A business impact analysis (BIA) normally comprises of two stages. The first stage is to (i) identify potential scenarios that may interrupt a licensee's services over varying periods of time and (ii) identify the minimum level of critical services that must be maintained in the event of a prolonged service interruption.

(c) The second stage of a BIA is a time-frame assessment. It aims to develop key realistic, measurable and achievable recovery time objectives: (1) maximum tolerable downtime (MTD) to recover and resume the minimum levels of critical services, (2) recovery time objective (RTO) to recover critical IT resources and (3) recovery point objective (RPO) to recover data.

(d) A BIA should be regularly reviewed, taking into account lessons to be learnt from technology risk incidents and changes in business environment (e.g. changes in technology applications, provision of new products/services, notable increase in business scale).

Recovery strategies

(e) A set of recovery strategies should be put in place, which should be clearly documented, thoroughly tested, and regularly drilled to ensure achievement of recovery targets.

(f) A crucial element of service recovery is robust record management. A licensee should put in place effective measures to ensure that all business records, in particular user records, can be timely restored in case they are lost, damaged, or destroyed. It is also crucial for a licensee to allow users to access their own records in a timely manner.

(g) In determining a licensee's levels of minimal services and the recovery objectives, it should take into account a host of relevant factors, including but not limited to interdependency among critical services/systems, expectations of users and other stakeholders in terms of speed, stability, and reliability of its services, legal and reputational risk implications.

Business continuity plan (BCP)

(h) Among other things, it is generally expected that a BCP comprises (i) detailed procedures to trigger service recovery strategies, (ii) escalation procedures and crisis management protocol (e.g. set up of a command centre, timely reporting to the HKMA) in case of severe or prolonged service disruptions, (iii) proactive communication strategies (e.g. customer notification, media response), (iv) updated contact details of key personnel involved in BCP, which should be shared with the HKMA; and (v) assignment of primary and alternate personnel responsible for recovery of critical systems.

Alternate sites for business and IT recovery

(i) Site selection

(i) A licensee should examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of the alternate sites to primary sites. Alternate sites should be sufficiently distanced to avoid being affected by the same disaster.

(ii) A licensee's alternate site should be readily accessible, installed with appropriate facilities and available for occupancy within the time requirement specified in its BCP. Appropriate physical access controls should be implemented. A licensee should also pay particular attention to the transportation logistics for relocation of operations to alternate sites.

(j) Alternate sites for IT recovery

(i) Alternate sites for IT recovery should have sufficient technical equipment, including communication facilities, of appropriate model and capacity to meet recovery requirements. A licensee should consider arranging telecommunication links from its alternate sites to the alternate sites of key external parties whose primary sites

are close to licensee's primary business locations.

(k) Alternate sites provided by vendors or other institutions

(i) A licensee should avoid placing excessive reliance on external vendors in providing BCP support. A licensee should satisfy itself that such vendors do have the capacity to provide the services when needed and the contractual responsibilities of the vendors, including the lead-time, types of support and capacity, are clearly specified.

(ii) If a licensee is reliant on shared computing services provided by external providers, such as cloud computing, to support its disaster recovery, it should manage the risk associated with these services. Please refer to the section on Outsourcing Management for guidance on IT outsourcing.

Guideline 7.4.2	*The board and senior management of a licensee have the ultimate responsibility for BCM and the effectiveness of their business continuity plans. It should ensure that BCM programs are duly implemented and taken seriously by all levels of staff and that sufficient resources are devoted to implementing the plan.*
Additional guidance	In assessing whether the board and senior management of a licensee have discharged their responsibilities under Guideline 7.4.2, the HKMA will consider the following: **Board and senior management oversight** (a) Establishment of responsibility (i) Senior management of the licensee should establish clearly which function has the responsibility for managing the entire process of business continuity management (BCM), and ensure that it has sufficient resources and expertise. (b) Monitoring, reporting and approval (i) The BCM function should submit regular reports to the Board and senior management on the testing of its business

continuity plan (BCP). Any major changes to the BCP should also be reported to the senior management.

(ii) The Board and senior management should ensure adequate audit coverage for its BCP to determine whether the plan is realistic and remains relevant, and whether it adheres to the policies and standards established by the licensee.

(iii) Given the importance of BCM, the Chief Executive of a licensee should prepare and sign-off a formal annual statement submitted to the Board on whether the recovery strategies adopted are still valid and whether the documented BCPs are properly tested and maintained.

Implementation of Business Continuity Plan

(c) Testing and rehearsal

(i) A licensee is expected to conduct testing of its BCP at least annually. Senior management, primary and alternate relevant personnel should participate in the annual testing to familiarize themselves with their recovery responsibilities.

(ii) All BCP related risks and assumptions must be reviewed for relevancy and appropriateness as part of the annual planning of testing. Formal testing documentation (including test plan, scenarios, procedures and results) should be produced. A post mortem review report should be prepared for formal sign-off by senior management. If testing results indicate a weakness or gap in the BCP, the plans and recovery strategies should be updated to remedy the situation.

(d) Periodic maintenance

(i) A licensee should have formal change management procedures to keep its BCP updated in respect of any relevant changes. In the event that a plan has been

activated, a review should be carried out once normal operations are restored to identify areas for improvement. If vendors are needed to provide vital recovery services, regular reviews of the service level agreements should be conducted.

(ii) Business and support functions, with the assistance of the BCM function, should review their BIA and recovery strategies on an annual basis to confirm the validity of the BCP requirements.

(iii) The contact information for key staff, counterparties, users and service providers should be updated as soon as possible when notification of changes is received.

(iv) Copies of the BCP document should be stored at locations separate from the primary site(s). A summary of key steps to take in an emergency should be made available to senior management and other key personnel and kept in multiple locations.

8. Business Practices and Conduct

Guideline section 8.2 - Standard of conduct and business practices

Guideline 8.2.3	*A licensee should ensure that it adopts, and if needed develops, good business practices that can demonstrate its standard of conduct.*
Additional guidance	(a) In typical situations, the following business practices should at least be adopted: (i) Due diligence should be performed by a licensee to ensure that all promotional materials it issues are accurate and not misleading; (ii) A licensee may use its websites and mobile apps to provide links to e-commerce portals and other online merchants. When providing such links, the licensee should carry out due-diligence on the e-commerce portals and merchants acquired to ascertain they are *bona fide* companies conducting legitimate business so as to manage reputation risk; and (iii) Websites or apps of a licensee may provide hyper-links to other websites which offer advisory and/or sale of financial products and services provided that the licensee has sought external legal opinion to ensure that the arrangements comply with all relevant legal and regulatory requirements. The licensee should indicate such products and services are provided by third parties, and insert disclaimers on its websites or apps that such hyper-link is not related to its SVF business and that the relevant products and services are not endorsed by the licensee or the HKMA or any other authorities.
Guideline 8.2.4	*A licensee is not allowed to provide interest payment or interest-like incentive scheme based on the volume of float.*

Additional guidance	(a)	For the avoidance of doubt, a licensee may offer incentive schemes which are not based on the volume of float, e.g. schemes that are transaction-based. Nevertheless, it should ensure and demonstrate that such schemes have a viable and sustainable business case. Among other things, a licensee is expected to conduct rigorous analysis to ensure that the budgetary implications of its schemes are under tight control.

Guideline section 8.3 - Schemes and operating rules

Guideline 8.3.1	*The operating rules of an SVF scheme should be fair to all parties concerned. A licensee should operate its SVF scheme in strict accordance with the relevant operating rules.*	
Additional guidance	(a)	The operating rules of an SVF scheme should cover the complete chain of an SVF's operation including but not limited to user account opening and maintenance, merchant acquisition and contractual relationships with business partners, pre-transaction, payment authorization and post-transaction processes.
	(b)	If a licensee intends to engage business partners (e.g. merchant acquirers to procure local or overseas merchants), it should ensure that the arrangement with business partners will not compromise its obligations under the PSSVFO in respect of ensuring safe and efficient operation of the SVF scheme, among other things:
		(i) The licensee should conduct due diligence on business partners to carefully assess the risks involved before engaging the business relationship, and to put in place adequate control mechanism to mitigate the risks identified;
		(ii) Where the licensee would rely on business partner(s) to conduct certain assessments or activities, such as but not limited to performing regulatory compliance analyses and/or engagements for ensuring the relevant initiative would be compliant with applicable laws, rules, regulations

or requirements, the licensee should take appropriate steps to confirm that the work is properly conducted and is clearly documented, and available for the HKMA's assessment as necessary.

(iii) The licensee should be satisfied that the contractual relationship between itself and business partners is clearly constructed and enforceable with well-defined division of duties and liabilities supported by well-documented service level agreements, and that there are necessary safeguards in its contractual relationship with the business partners to ensure the operational safety and efficiency of the SVF scheme. In case of merchant acquisition, the licensee should also ensure that the contractual relationship between merchant acquirers and merchants fulfill the above requirements;

(iv) The licensee should impose appropriate controls and oversight over the business arrangements with its business partners (e.g. in case of merchant acquirers, to ensure that they have proper systems in place for settlement of funds with the merchants) and for mitigation of any potential money laundering and terrorist financing risks; and

(v) The licensee should ensure that the arrangement of engaging business partners is compliant with PDPO and also observes the relevant supervisory guidelines on data protection in order to safeguard the interest of its users.

Guideline 8.3.4	*A licensee should set out and explain clearly the key features, risks, terms and conditions, and applicable fees, charges and commissions of its schemes, facilities, services and products. Such details should be effectively communicated and made available to the relevant users, including merchants. Additional disclosures, including appropriate warnings, should be developed to provide information commensurate with the nature, complexity and risks of the schemes, facilities, services and products. In particular, the related contract with a user under a scheme should state clearly and prominently the amount of the fee and*

	charge payable and the circumstances in which the fee and charge becomes payable.
Additional guidance	(a) A licensee should set out clearly their personal data policies and practices in a manner that can fulfil the requirements under the PDPO as well as any relevant codes of practice, guidelines or best practice issued by the Office of the PCPD from time to time. (b) Where appropriate, a licensee should provide a facility for users to confirm that they have read the key information and disclosures relating to the use of its services/products before they sign up for the services/products. For example, a confirmation facility may be provided on a web page containing the key disclosures to allow users to declare, by clicking on the facility, that they have read the disclosures therein.
Guideline 8.3.5	*A licensee should be solely responsible for the robustness of its SVF scheme and as such it should bear the full loss of the value stored in a user account where there is no fault on the part of the user.*
Additional guidance	(a) A licensee is expected to observe Guideline 8.3.5 in all circumstances. Unless it can be demonstrated that a user acts fraudulently, with gross negligence (such as failing to safeguard properly his/her card(s), device(s) or secret code(s) for accessing the SVF services/products) or fails to inform the licensee as soon as reasonably practicable after the user finds or believes that his/her account (such as the card(s), device(s) or secret code(s) for accessing the SVF services/products) has been compromised, lost or stolen, or that unauthorized transactions have been conducted over his/her account, he/she should not be responsible for any direct loss suffered by him/her as a result of unauthorized transactions conducted through his/her account.

Guideline section 8.4 - Complaints handling

Guideline 8.4.2	*The complaint management system of a licensee should be comprehensive, transparent, accessible to SVF users and easy to invoke, fair and impartial, consistent in its approach to the provision of redress, flexible and efficient, and able to maintain appropriate confidentiality, keep sufficient records, resolve complaints, identify and remedy the problems revealed by the complaints and provide appropriate feedback to the HKMA.*
Additional guidance	In assessing a licensee's compliance with Guideline 8.4.2, the HKMA will generally consider, among other things, the following taking into account the scale and complexity of a licensee's business: (a) There are in place comprehensive and transparent complaints handling policies to the effect that complaints can be dealt with in a prompt, objective, equitable, consistent, and confidential manner; and that there are appropriate management controls to monitor compliance and proper implementation of the relevant policies and procedures; (b) Information on how and where to lodge complaints are clear, visible, accessible and comprehensible to complainants. There are in place sufficient channels and means for complainants to lodge complaints; and that acknowledgement of complaints, follow up actions, feedbacks and outcomes are duly communicated to the complainants in an adequate and timely manner; (c) Effective policies and procedures are in place to ensure the privacy of complainants. Among other things, clear procedures should be in place to protect the identity of complainants, and information relating to complaints can be strictly restricted to responsible staff on a need to know basis; (d) Sufficient resources, including staffs with relevant skills, training, authorities and independence are devoted to ensure that complaints are handled and followed up effectively and efficiently; and that there are effective mechanisms for senior management of the licensee to monitor the progress and process

of complaints handling;

(e) Where complaints are upheld, satisfactory remedies and redress are provided to the complainants within a reasonable period of time; and that effective systems are established to allow remedies and redress to be determined taking into account circumstances and natures of the complaints; and

(f) There are in place clear accountabilities for complaints handling, and that complaints are used as sources for implementing further organizational and operational improvements. Comprehensive and accurate records of facts, correspondences and relevant details of complaints and handling processes are maintained confidentially for an appropriate period of time. Such records should be made available to the HKMA upon request.

Annex

Good Practices for IT Controls

Development and acquisition of information systems

(a) Project management

(i) A general framework for management of major technology-related projects, such as in-house software development and acquisition of information systems is established. This framework, among other things, specifies the project management methodology to be adopted and applied to these projects.

(b) Project life cycle

(i) A full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems is adopted and implemented.

(ii) The project life cycle methodology defines clearly the roles and responsibilities for the project team and the deliverables from each phase.

(iii) Where a licensee acquires software package from vendors, a formal software package acquisition process is established to manage risks associated with acquisitions, such as breach of software licence agreement or patent infringement. Ensure that on-going maintenance and adequate support of software packages are provided by the software vendors and are specified in formal contracts.

(iv) Conduct quality assurance review of major technology-related projects by an independent party, with the assistance of the legal and compliance functions if necessary.

(c) Security requirements

(i) Define security requirements clearly in the early stage of system development or acquisition as part of business requirements, built during program development, tested and implemented.

(d) Coding practice

(i) Develop guidelines and standards for software development with reference to industry generally accepted practice on secure development.

(ii) Implement source code reviews (e.g. peer review and automated analysis review), which could be risk-based, as part of software quality assurance process. Identify and fix system vulnerabilities and non-compliance with coding practices before a system goes live.

(e) System testing, acceptance and deployment

(i) Establish a formal testing and acceptance process to ensure that only properly tested and approved systems are promoted to the production environment. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

(ii) Maintain segregated environments for development, testing and production purposes. System testing and user acceptance testing (UAT) are properly carried out in the testing environment.

(iii) Production data are not used in development or acceptance testing unless the data has been desensitised and prior approval from the information owner has been obtained.

(iv) Penetration testing by an independent party is properly conducted before the system goes live.

(f) Segregation of duties

(i) Segregation of duties among IT teams are properly maintained. Developers are unable to get access to production libraries and promote programming code into the production environment. Vendor accesses to the UAT environment, if necessary, are closely monitored.

(g) End-user computing

(i) An inventory of end-user developed software is maintained and, where necessary, control practices and responsibilities with respect to end-user computing to cover areas such as ownership, development standard, data

security, documentation, data/file storage and backup, system recovery, audit responsibilities and training are established.

IT service support

(h) Problem management

(i) A problem management process to identify, classify, prioritise and address all IT problems in a timely manner is established. Clear roles and responsibilities of staff involved in the problem management process are established. A trend analysis of past incidents is performed regularly to facilitate the identification and prevention of similar problems.

(i) Change management

(i) Typically, change management is the process of planning, scheduling, applying, distributing, tracking changes and post implementation verification of the changes made to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. A formal change management process is developed to ensure the integrity and reliability of the production environment and that the changes are proper and do not have any undesirable impact on the production environment. Formal procedures for managing emergency changes (including the record keeping and endorsement arrangement) are also established to enable unforeseen problems to be addressed in a timely and controlled manner.

(j) Security baseline standards

(i) Control procedures and baseline security requirements, including all configurations and settings of operating systems, system software, databases, servers and network devices etc., are adequately and accurately documented. Periodic reviews on the compliance of the security settings with the baseline standards are performed.

IT service delivery

(k) Internal service level agreement

(i) A service level agreement with business units covering system availability and

performance requirements, capacity for growth, and the level of support provided to users is formulated by the management of IT functions. Adequate procedures are established by the responsible IT functions for managing the delivery of the agreed technology support and services.

(l) System availability and capacity management

(i) An effective process is implemented to ensure that the system availability and performance is continuously monitored and exceptions are reported in a timely and comprehensive manner.

(ii) Capacity planning is extended to cover backup systems and related facilities in addition to the production environment.

IT operation

(m) Job scheduling

(i) The initial schedules and changes to scheduled jobs are appropriately authorized. Procedures are in place to identify, investigate and approve departures from standard job schedules.

(n) Vulnerability and patch management

(i) A combination of automated tools and manual techniques is deployed to regularly perform comprehensive vulnerability assessments. For web-based external facing systems, the scope of vulnerability assessment includes common web vulnerabilities.

(ii) Patch management procedures are formulated to include the identification, categorisation, prioritisation and installation of security patches. To implement security patches in a timely manner, the implementation timeframe for each category of security patches is defined based on severity and impact on systems.

(o) Security monitoring and reporting

(i) Security monitoring tools are implemented to

- retain system, application and network device logs to facilitate investigation when necessary in accordance to the licensee's defined

log retention policy;

- monitor critical configurations and security settings to identify unauthorized changes to these settings and block anomalies on IT assets, e.g. abnormal user behaviors, unusual system processes and memory access and malicious call backs to devices;

- perform real-time analysis on security logs and events for critical systems and applications, to promptly detect any potential attacks; and

- any suspicious or confirmed breach must be passed to incident handling team for proper handling, escalation and reporting.

(p) IT facilities and equipment maintenance

(i) IT facilities and equipment are maintained in accordance with the industry practice, and suppliers' recommended service intervals and specifications to ensure the facilities and equipment are well supported.

(q) Mobile computing

(i) Where a licensee provides mobile devices for its employees, policies and procedures covering, among others, requisition, authentication, hardening, encryption, data backup and retention are established.

(ii) Where a licensee is considering adopting Bring Your Own Device (BYOD) at work, the scope of BYOD adoption, the information to be accessed and the confidentiality of the data to be accessed are specified, and risk assessment is performed according to the TRM framework set forth in this Practice Note.

Network and Infrastructure management

(r) Network management

(i) Overall responsibility for network management is clearly assigned to individuals who are equipped with expertise to fulfil their duties. Network standards, design, diagrams and operating procedures are formally documented, kept up-to-date, communicated to all relevant network staff and reviewed periodically.

(ii) Communication facilities that are critical to the continuity of network services are identified. Single points of failure are minimised by automatic re-routing of communications through alternate routes should critical nodes or links fail.

(s) Network security

(i) A secure network infrastructure to support its systems is established. To prevent insecure connections to the licensee's networks, procedures concerning the use of networks and network services are established and enforced. These cover:

- the available networks and network services;
- authorization procedures for determining who is allowed to access particular networks and network services; and
- controls and procedures to protect access to network access points, network connections and network services.

(ii) Segregating internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment is considered.

(iii) Regular reviews of the security parameter settings of network devices such as routers, firewalls and network servers are conducted to ensure that they remain current. Audit trails of daily activities in critical network devices are maintained and reviewed regularly. Network operational personnel are alerted on a real-time basis to potential security breaches.

(iv) Encryption technology and network monitoring tools, covering both external and internal networks, are properly implemented to protect sensitive information in internal networks, communication channels to third parties and external networks.

(t) Data Centre management

(i) Risk assessment is performed for data centres to identify security threats to and operational weaknesses in data centres, and also, assess the adequacy of safeguarding controls over the data centres.

(ii) Adequate security controls are implemented on physical access to licensee's data centres. Access rights are granted only if necessary and are regularly reviewed. Access to data centres are logged and regularly reviewed. Special attention is given for a licensee using multi-tenancy data centres, to prevent unauthorized access to IT equipment.

IT outsourcing

(u) IT outsourcing to overseas offices

(i) Where a licensee is reliant upon or work with its overseas offices (e.g. parent company, subsidiaries, head offices or other regional offices of the same group) with regard to outsourcing arrangements on certain IT controls or support activities, the respective responsibilities of the local and overseas offices in these areas are clearly set out in the relevant documents (e.g. policies, procedures, outsourcing and/or service level agreements).

(v) Management of other technology service providers

(i) Apart from technology outsourcing, a licensee may be reliant on some outside technology service providers in the provision of technology-related support and services (e.g. telecommunications and network operators). Guidelines on how to manage different kinds of major outside technology service providers including the selection process of service providers, the process for approving material exceptions, and the need to avoid over-reliance upon a single technology service provider in critical technology services are established.

(w) Special attention on cloud computing

(i) As cloud computing is generally considered a type of IT outsourcing, a licensee intending to procure or have procured cloud computing services would adhere to the relevant guidance paper, as well as any relevant guidelines or best practices issued by Government bodies from time to time.