This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To provide guidance to AIs on the risk management of e-banking

Classification

A statutory guideline issued by the MA under the Banking Ordinance §7(3)

Previous guidelines superseded

TM-E-1 "Risk Management of E-banking" (V.3) dated 24.10.19

TM-E-1 "Risk Management of E-banking" (V.2) dated 02.09.15

Circular "Security Controls related to Internet Banking Services" dated 26.05.16

Application

To all AIs

Structure

1. Introduction

1.1 Background

1.1.1 This module sets out guidance on the sound risk management principles and practices applicable to AIs' electronic banking services ("e-banking" as defined in subsection 1.2 below). It has taken into account latest developments in the banking industry and in relevant technologies as well as supervisory guidance used in other major jurisdictions so as to facilitate the further development of e-banking in Hong Kong while also enhancing the industry's risk management controls in this area.

1.2 Types of e-banking

1.2.1 For the purpose of this module, e-banking refers to financial services (which can be transactional, enquiry or payment services) provided to personal or business customers and delivered over the Internet, wireless networks, automatic teller machines (ATMs), fixed telephone networks or other electronic terminals or devices.

1.2.2 Accordingly, e-banking includes: (i) Internet banking[1]; (ii) contactless mobile payments[2]; (iii) financial services delivered through self-service terminals[3]; and (iv) phone banking[4]. Except for certain guidance in this module on controls over payment card[5] transactions

[1] Internet banking refers to financial services delivered over the Internet to customers' devices including personal computers and mobile devices.

[2] Contactless mobile payments refer to the use of contactless or wireless technology to transmit payment transaction information between the customer's mobile device and the payee.

[3] Self-service terminals refer to interactive terminals (including ATMs, cash deposit machines (CDMs), cheque deposit machines and virtual teller machines) which are used by AIs to provide financial services.

[4] Phone banking refers to banking services provided through telephone line or mobile telecommunication network, covering both manned and Interactive Voice Response (IVR) phone banking services. For the purpose of this module, phone banking does not include the provision of banking services for the purpose of sales promotion or activity notification/call-back confirmation, or by a designated staff member (e.g. a relationship manager) who knows the relevant customer very well.

[5] Payment card refers to any cards (whether physical or virtual) that allow cardholders to make payment for goods and services.

(see subsection 7.6 below), this module does not cover other controls for managing the risks associated with AIs' credit card business (see in this regard CR-S-5 "Credit Card Business"). This module also does not intend to cover controls related to electronic terminals provided to merchant clients by merchant acquiring AIs, although some control practices in this module may also be relevant to addressing the risks associated with those services. Further, services where AIs allow customers to send their instructions through emails or faxes are not covered because such services should not be regarded as e-banking.

1.3 Supervisory objective and approach

1.3.1 The HKMA's supervisory objective is to promote a safe and transparent regulatory environment for e-banking, thereby maintaining public confidence in e-banking at large and fostering its further development. In this connection, the HKMA works periodically with the banking industry to develop sound risk management principles and practices that are commensurate with the associated risks of e-banking in order to mitigate the risk of fraud as well as other key risks.

1.3.2 The HKMA adopts a risk-based and technologically neutral supervisory approach (see also SA-1 "Risk-based Supervisory Approach") to supervising AIs' e-banking services. The HKMA undertakes onsite examinations and performs various off-site supervisory reviews and other activities to assess how AIs manage the risks of e-banking.

1.4 Applicable risk management principles

1.4.1 Given that e-banking involves the delivery of financial services through technological means, both general risk management principles applicable to the provision of the underlying financial services and typical technological controls are applicable to e-banking. This module does not repeat the HKMA's general guidance in these areas but rather elaborates on how the relevant risk management measures may be applied or refined in the case of e-banking for different types of

customers[6].

1.4.2 AIs should use a risk-based approach to managing the risks associated with e-banking. In this connection, AIs should comply with the requirements in this module and should also make reference to other relevant Supervisory Policy Manual modules and HKMA guidance issued from time to time. AIs are also expected to refer to the Code of Banking Practice (the "Code") and any relevant guidelines issued by the banking industry associations on applicable risk management principles.

2. Major risks inherent in e-banking

2.1 Operational risk

2.1.1 Operational risk is a key risk associated with e-banking, usually in terms of frauds, cyber threats, information leakages, service disruptions or system processing errors. This is because e-banking usually entails (i) provision of financial services to a sizeable group of customers over a network or via terminals or devices that are beyond AIs' direct control or that are not protected by the usually more stringent physical security controls generally found within AIs' premises; (ii) reliance on multiple service providers (including the vendors of the relevant terminals or devices, telecommunication network operators, other service providers operating or supporting the e-banking computer systems or related networks, overseas offices or even other banking institutions); (iii) relatively new or complicated system architecture or processing logics; (iv) real-time transactions that are effected around the clock. Furthermore, the threat of attack and fraud related to e-banking and the form it may take are evolving over time, and hence the nature of operational risk is dynamic.

[6] For the avoidance of doubt, the guidance set out in this module should be observed by AIs in respect of e-banking services for both personal and business customers where applicable.

2.2 Reputation and legal risk

2.2.1 In the light of the heightened operational risk mentioned above, AIs may easily be exposed to increased reputation risk arising from operational incidents such as significant security breaches, data leakages, e-banking system slowdown/disruptions or malfunctions, or the inability of AIs' alternate channels to cope with the impact caused by any disruptions. Reputation risk will also arise if AIs fail to properly deal with customers' complaints and disputes related to e-banking. In the event that operational incidents or disputes lead to legal actions taken by the affected customers or other relevant parties, AIs would face reputation and legal risk.

2.2.2 In addition, AIs are subject to potential reputation and legal risk if they offer e-banking services involving transmission of sensitive customer information to and from other institution(s) (which could be outside Hong Kong), storage of AIs' customer data by other institutions, or the potential need to deal with customer disputes or losses that may be related to, or caused by, other institutions or events taking place in other jurisdictions. AIs should also be mindful that e-banking provides channels for their customers / potential customers to access their services / products and this may present a similar range of risks as other channels or render the AIs exposed to additional risks depending on the scope of services offered through these channels. For example, an AI may be exposed to additional legal and reputation risk if its e-banking services increase its vulnerability to the abuse of money laundering and terrorist financing (such as facilitating anonymity), or if its e-banking services involve cross-border activities (e.g. solicitation of deposits or business from overseas customers and cross-border funds transfers) while the overseas authorities regard the service as targeting overseas residents and requiring authorization in their jurisdictions.

2.3 Risks associated with underlying financial services

2.3.1 Apart from the risks driven mainly by the use of technologies or the electronic channels used in e-banking, AIs also face the risks associated with the underlying financial services delivered through e-banking. For instance, a lending function offered through Internet banking will expose AIs to the relevant credit risks. Similarly, AIs are subject to essentially the same risks (such as operational, reputation and legal risk) arising from a securities brokerage function if they offer such function via Internet banking.

2.3.2 Among the risks related to the underlying financial services delivered through e-banking, AIs should pay particular attention to the possible implications of e-banking services for their liquidity risk management. Specifically, e-banking services may allow customers to transfer large sums of funds to bank accounts in other institutions more easily compared to the traditional way of banking. This could result in potentially different customer behaviour, especially in times of stress.

3. Risk governance of e-banking

3.1 Board and senior management oversight

3.1.1 It is the primary responsibility of AIs to ensure that the risks posed by e-banking are properly managed and to educate and protect their customers. In the light of the inherent operational, reputation and legal risk as well as potential liquidity risk associated with e-banking, an AI's Board[7], or its designated committee, and senior management should exercise effective oversight of the risk management processes undertaken by both relevant business lines and support functions (especially the IT function) relating to e-banking in

[7] For the purpose of this module, the responsibility for the oversight of e-banking in respect of the Hong Kong operations of an overseas incorporated AI would rest with its local senior management, under the monitoring of its head-office or regional head-quarters, especially if its e-banking requires material support and involvement of the AI's overseas offices.

order to ensure that:

(i) the risks associated with e-banking are fully understood and that adequate risk management measures are taken when introducing or enhancing e-banking and thereafter, as there might be changes in risk over time especially as technologies evolve. In this connection, the AI's Board and senior management should attach priority to defining clear ownership of risks and promoting a strong risk culture, and devote sufficient financial resources in maintaining adequate staffing resources and expertise to manage the risks inherent in e-banking. In the event that the AI does not have the required resources or expertise to implement the required risk management controls, it should not launch or offer e-banking;

(ii) the AI complies with all relevant supervisory requirements/guidance issued by the HKMA or other relevant authorities as well as industry associations from time to time, including the risk management principles and practices set out in this module and other relevant modules, when introducing or enhancing its e-banking; and

(iii) the AI has an adequate system of checks and balances. Where material control deficiencies are identified, appropriate follow-up actions should be considered and monitored by the Board or senior management.

3.2 Accountability and staff competence in the three lines of defence

3.2.1 Since risk management in relation to e-banking is generally complicated and evolving (especially in respect of operational risk), it is vital for an AI to ensure that:

(i) the management and staff of the relevant business lines and support functions (i.e., the first line of defence) are accountable for, and

competent in, assessing and monitoring the relevant risks and implementing the required risk management controls; and

(ii) in addition, the AI should clearly specify the accountability of the management and staff of its second line of defence (e.g. risk management function, compliance function) in evaluating the adequacy of the risk management controls implemented by the first line of defence, as well as the role of the third line of defence (normally the internal audit function) in auditing the relevant risk management controls. It is important for the Board and senior management to support the development of the technical competence and knowledge required by the second and third lines of defence for such check and balance functions accordingly.

3.3 Independent assessment and penetration tests

3.3.1 As part of the risk governance for e-banking, AIs' senior management should establish clear policies and accountability to ensure that a rigorous independent assessment is performed before the launch of any new electronic delivery channel of e-banking service, or a major enhancement to existing services. The purpose of the independent assessment is to validate whether the e-banking service complies with applicable regulatory guidance and whether sufficient risk management controls are actually in place in relation to the service or enhancement concerned. In this connection, the AI's policy framework for independent assessment should ensure that, among others:

(i) the senior management designate which function(s) (e.g. the main business line sponsoring the e-banking service, the risk management function or the internal audit function) to be responsible for the quality of, and undertaking proper follow-up actions arising from e-banking independent assessment. All issues with material risk and associated impact identified by independent assessment should be

satisfactorily resolved or accepted by senior management with sufficient justifications before the launch of the service or enhancement. For issues with material risk but accepted by senior management, they should be subject to a mechanism of periodic re-evaluation so as to ascertain whether the acceptance remains appropriate;

(ii) the scope of independent assessment covers, at a minimum, an objective evaluation (which may be risk-based) of whether adequate risk management controls have been implemented for the e-banking service in question, including those applicable controls set out in this module (focusing on relevant controls under sections 4 to 9) and other applicable HKMA and industry guidelines and circulars that are relevant to the underlying financial services and the electronic delivery channel concerned. Where relevant, the independent assessment should cover all relevant systems or processes outsourced to service providers within or outside the banking group. That said, the scope of the independent assessment may be appropriately adjusted if certain controls, systems or processes have been assessed or audited within a reasonable period of time prior to the independent assessment with respect to the risks involved; and

(iii) independent assessment is performed by trusted assessors with the necessary expertise in the underlying financial services and/or electronic delivery channel, and who are independent from the parties that design, implement or operate the e-banking service. Moreover, the assessors should be able to report their findings freely and directly to the Board (or its designated committee(s)) and senior management of the AI whenever there is a need. So long as these conditions can be met, the assessors may come from any function, particularly the second line of defence (e.g. risk

management function) or the internal audit function of the AI or the banking group, an external auditor acceptable to the AI (e.g. including those appointed by outsourcing service providers) or any other third-party consultants. Where multiple assessors are needed in the independent assessment (e.g. when the assessor for assessing a third-party service provider is different from the assessor who reviews the AI's own systems and controls), the responsible function(s) as defined in subsection 3.3.1(i) should ensure that there is no gap among the scope of assessment performed by different assessors. In general, items to be reported in the independent assessment should cover, at a minimum, the areas specified in Annex A, and the report should be submitted to the HKMA upon request.

3.3.2 If an AI's policy framework for independent assessment does not include penetration tests, the senior management should further ensure that regular penetration tests are performed by qualified independent parties. For the purpose of this module, a penetration test should assess, at the minimum, the AI's Internet banking and any financial services delivered over the Internet or via a wireless network (covering enquiry-only services and relevant outsourced systems) annually. Penetration tests should be carefully planned and carried out so as not to unduly disrupt the AI's production systems/channels.

3.3.3 Apart from independent assessment and penetration tests mentioned in subsections 3.3.1 and 3.3.2, formal risk assessment should be conducted periodically, at least on an annual basis, to ensure that adequate risk management controls have been implemented for Internet banking and financial services delivered over the Internet. The risk assessment should take into account objective analysis of any material change to the risk profile of the financial services being provided or the AI's e-banking system, emerging vulnerabilities and other risks related to the electronic delivery channels concerned, etc. The party responsible for

performing such risk assessment should have sufficient expertise in the emerging risks posed by the e-banking service concerned. Moreover, the risk assessment result should be endorsed by designated senior officer and any material issues identified in the assessment should be rectified on a timely basis.

4. Customer security

4.1 Authentication of customers

4.1.1 AIs should adopt an effective authentication method to verify the identity of a customer when he/she opens an account of e-banking service or accesses his/her account. AIs should also ensure the ongoing effectiveness of the authentication method, having regard to emerging cyber threats and fraud risk. They should maintain the capability to implement multiple authentication methods and establish a mechanism to swiftly deploy alternative authentication methods to cope with evolving fraud risk.

4.1.2 In general, two-factor authentication [8] (2FA) of customers should be implemented for e-banking channels that allow high-risk transactions (See paragraph 4.1.4).

4.1.3 AIs should put in place adequate controls related to the strength of the password including a Personal Identification Number (PIN) (e.g. certain password requirements that can increase the difficulty of a successful brute-force attack). Effective measures should be implemented to counter automated brute-force attacks and disallow repeated login attempts using invalid passwords. AIs should also periodically remind their customers whose passwords remain unchanged for a prolonged period to change their passwords. Moreover, AIs should implement appropriate segregation of duties and security measures to ensure any password generated, re-issued or reset by AIs would not be disclosed or leaked

[8] Two-factor authentication refers to the use of two out of the three types of factors (i.e. (i) something a customer knows; (ii) something a customer has; and (iii) something a customer is).

during the generation and delivery.

4.1.4 For Internet banking, AIs should require 2FA at least once to authenticate customers' identity for each login session before performing high-risk transactions. High-risk transactions should cover, at least, high-risk funds transfers, which include:

(i) funds transfers to third-party payees that have not been registered by the customers;

(ii) bill payments to merchants that have been classified by AIs as high-risk merchants[9] but where the payees have not been registered by the customers; and

(iii) transactions that effectively allow online transfers[10] of customers' eligible monetary or non-monetary benefits or interests (e.g. credit card rewards points), directly or through conversion/redemption (including via AIs' corporate websites), to third parties that have not been registered by the customers.

4.1.5 While the general requirement is that at least one time of 2FA should be conducted before performing high-risk transactions, AIs should consider stepping up customer authentication control (e.g. requiring the customer to undertake another authentication using 2FA or transaction signing before performing each such transaction) having regard to the riskiness of the transactions.

4.1.6 If a high-risk transaction is considered to be suspicious or otherwise related to fraudulent activities (e.g. large-value funds transfers shortly after device binding), AIs should request customers to provide an additional

[9] AIs should establish an effective and proper due diligence process to assess and determine whether a merchant should be classified as a high-risk merchant (e.g. credit cards lenders and other money lenders, securities brokers, money changers and the Telebet services). Regular assessment should also be conducted on these merchants to ensure that the assigned categories remain appropriate.

[10] It is acceptable that no 2FA is used to authenticate a customer's identity when the monetary value related to a transfer does not exceed the AI's prudent cap(s) for small-value funds transfers via Internet banking (see subsection 6.1.1).

confirmation.

4.1.7 If suspicious e-banking activities are detected (e.g. access from suspicious IP addresses or device IDs), AIs should verify the identity of the person operating the account at a point of time outside the person's expectations ("ambush authentication"). An ambush authentication should be triggered following a risk-based approach. In cases where the person fails to pass the ambush authentication more times than the threshold defined by AIs, appropriate actions, such as account lock-out, issuing alerts to customers and contacting them, should be taken.

4.1.8 AIs should ensure that registration of a payee in a high-risk transaction should only be allowed through secure channels with adequate identity checks conducted by AIs. However, AIs may regard small-value funds transfers (see subsection 6.1.1 below) as not being high-risk transactions.

4.1.9 AIs should perform adequate identity checks when any customer requests a change to the customer's account information (including resetting or reissuing of account password) or contact information (e.g. e-mail address, contact phone number, correspondence address) that are used by the customer to receive important information. AIs should take measures to prevent and detect possible malfeasance or frauds related to these changes.

4.2 Notifications sent to customers

4.2.1 To facilitate customers' timely detection of unauthorized transactions that may arise as a result of fraudulent activities related to e-banking channels, AIs should, as far as practicable, notify customers immediately via an effective channel once the customers initiate transactions that are considered as of higher risk. Each such notification message should contain the transaction details, including among others, the transaction type, partial information about the payee and transaction amount, if the information is available and relevant.

4.2.2 AIs should also have in place effective monitoring arrangements to identify unusual e-banking activities (e.g. significant change in geographical locations within a short period of time, use of new devices and new login behaviour) and notify customers of these activities in addition to high-risk transactions. These notifications should be designed to aid customers in detecting suspicious activities over their bank accounts early.

4.2.3 If AIs are aware of any notifications that cannot be delivered to the customers concerned, they should use a risk-based approach to following up those situations.

4.3 Customer awareness and education

4.3.1 AIs should warn their e-banking customers of the customers' obligations to take reasonable security precautions to protect the devices and the authentication factors (e.g. passwords and authentication tokens) used by the customers in the e-banking services. AIs should also observe the relevant provisions set out in the Code when providing e-banking services to personal customers. Moreover, AIs should periodically provide advice to their e-banking customers regarding precautionary security measures. Such advice should be easy-to-understand, prominently displayed and regularly reviewed and updated. The advice should be delivered through multiple effective channels. AIs should ensure that sufficient advance guidance and training are given to officers who handle customers' enquiries related to the security precautions of e-banking.

4.3.2 In addition, AIs should manage the risk associated with fraudulent websites, malicious mobile applications (Apps), fake Internet banking Apps, phishing emails or similar scams which are designed to trick their customers into revealing sensitive customer information such as account numbers, Internet banking

passwords, one-time password[11] (OTP) or credit card information. In particular, AIs should search the Internet and Apps stores regularly for fake or suspicious websites or Apps. Whenever AIs become aware of fake or suspicious emails, websites, Apps or similar scams that might give the public the false impression that they originate from the AI or that their Apps can be downloaded from unofficial sources, or cases involving suspicious Internet banking login screens (e.g. pop-up windows requesting customers to input their credit card information) affecting multiple customers within a short period of time, AIs should consider and decide in a timely manner how to inform their customers and the public more widely and report the matter to the Hong Kong Police Force (the "Police"). If it is considered to be in the best interests of their customers, AIs should notify promptly their customers through issuing press releases (or other similarly effective means), and report the matter to the HKMA[12]. Besides, AIs should make attempts to remove the fake or suspicious items where practicable.

4.4 Customer protection

4.4.1 AIs should provide appropriate functions in Internet banking that enable customers to review and monitor their account activities, which should include the login date and time, geographical location and device information. The relevant Internet banking functions should permit customers to search for high-risk activities conducted over a reasonably long period in the past (which should normally be no less than 90 days).

4.4.2 AIs should offer a convenient and easily accessible channel (e.g. Internet banking or dedicated hotline) available at all times for customers to seek and obtain help with respect to possible unauthorized transactions

[11] OTP is a password that is valid for authentication of a single access attempt only so that even if this one-time password is captured by a fraudster, the password cannot be reused for subsequent authentication.

[12] In general, AIs are expected to issue their press releases as soon as practicable after they become aware of the scams, and report the cases to the HKMA immediately after the press releases are issued.

over their e-banking accounts.

4.4.3 AIs should provide a mechanism for customers to promptly suspend their e-banking accounts in cases where fraudulent or suspicious activities are detected. The mechanism may take the form of a dedicated hotline or an easily accessible function available on Internet banking. AIs should perform appropriately stringent customer authentication before any suspended accounts are reactivated.

4.4.4 AIs should seek to protect the interests of all types of customers when offering e-banking services to them. In particular, AIs should respect the spirit of the Treat Customers Fairly Charter (TCF) and comply with the Code when offering e-banking services to their personal customers. This includes, among others, that unless a customer acts fraudulently or with gross negligence such as failing to safeguard properly his device(s) or authentication factors (e.g. passwords and authentication tokens) for accessing the e-banking service, he or she should not be responsible for any direct loss suffered by him or her as a result of unauthorized transactions conducted through his or her account (please refer to the Code for details). As regards business customers, AIs should ensure that there are clear terms and conditions provided to them, which should cover customers' risks and responsibilities, precautionary security measures, procedures for handling customer disputes and liabilities in relation to unauthorized transactions. Customers should be made aware of these terms before they are provided with e-banking services.

4.4.5 Separately, AIs are reminded of the need to comply with the Personal Data (Privacy) Ordinance and any relevant codes of practice / guidelines or guidance issued or published by the Privacy Commissioner for Personal Data or the Office of the Privacy Commissioner for Personal Data (PCPD) from time to time.

5. System and network security for Internet banking

5.1 Confidentiality and integrity of information

5.1.1 AIs should adopt secure and internationally-recognised strong encryption algorithms[13] to protect the confidentiality of customers' information transmitted over external networks including the Internet, and highly sensitive information (e.g. this refers mainly to customers' login credentials such as e-banking passwords) kept in storage or sent over internal networks. Sound key management practices should also be in place to safeguard the relevant encryption keys. As the strength of encryption could be affected if outdated or weaker algorithms technologies are used, AIs should carefully evaluate the implementation of relevant encryption controls for e-banking from time to time, and improve or update the implementation whenever there is a need.

5.1.2 AIs should also implement sufficient controls to maintain and verify the integrity of the information processed by their Internet banking systems. For example, AIs should implement checks and controls in the application systems so as to reconcile data file balances after transaction updates and to check the integrity of data transmitted between different systems.

5.2 Internet infrastructure

5.2.1 AIs should establish a secure Internet infrastructure (including the design of the demilitarized zone and configuration of the relevant devices, as well as intrusion detection controls) to support their Internet banking system. Moreover, AIs should implement adequate security measures for the internal networks and network connections to external parties, and proper patch management procedures for systems and infrastructure components.

[13] If it is not practicable to implement internationally-recognized strong encryption algorithms, AIs should still implement similarly stringent encryption algorithms as an alternative and the algorithms should be subject to independent assessment.

5.3 Application system security

5.3.1 AIs should put in place an adequate level of application system security in respect of their Internet banking system, including any Apps, covering at least application design and development, testing and implementation. In this connection, AIs should make reference to sound industry practices[14] on application system security.

5.3.2 Before launching any Internet banking system or system changes, an adequate application system source code review, which could be risk-based, should be performed. The review should aim at identifying any non-compliance with the relevant application security standards, any source codes that may potentially pose or create security threats/loopholes or whether any malicious code has been embedded in the application system. Such review should be conducted by an appropriate party[15] with relevant expertise and the party should also be independent of the staff who developed the application system.

5.3.3 For Internet banking, AIs should put in place effective session management controls that disallow concurrent logins to an e-banking account, unless there is a genuine need. Key data, such as IP address, device type, and geographical location of the additional login attempts, should be logged for auditing and threat analysis purposes.

5.4 Threat monitoring and vulnerability assessment

5.4.1 AIs should establish a systematic monitoring process to closely monitor emergent security threats that are relevant to their Internet infrastructure, application systems and other relevant system components and

[14] An example is the Open Web Application Security Project (www.owasp.org).

[15] It would be acceptable if the code review is a peer review, assisted by relevant automated tools, performed by another designated member of the system development team so long as the reviewer appropriately documents the scope, approach and outcome of the peer review. If the application system is developed by a third-party vendor, the AI should be satisfied that the vendor has put in place an adequate code review process. Otherwise, the AI should conduct a code review of the application system provided by the vendor.

operations.

5.4.2 AIs should also utilize automated tools (supplemented by manual techniques if needed) to perform periodic vulnerability assessment to detect security vulnerabilities in their Internet infrastructure and relevant Internet banking systems.

5.4.3 AIs should adopt a risk-based approach to addressing the risks arising from the security threats or vulnerabilities identified.

6. Controls related to services offered via Internet banking or the Internet

6.1 Funds transfers

6.1.1 As mentioned in subsection 4.1, AIs should implement 2FA to authenticate the customer's identity before effecting a high-risk funds transfer transaction. Nevertheless, AIs also have the flexibility to offer a service where small-value funds transfer transactions to unregistered payees are not regarded as high-risk transactions. In this case, those small-value funds transfers have to be subject to at least a transaction limit defined by the customer and should be bound by a cap determined by AIs. AIs should also clearly communicate to customers the risk implications of the transaction limit(s) especially when AIs provide such small-value funds transfer service to customers, or when customers set or increase the limit(s). To further prevent frauds from making use of such a service without the knowledge of the customers, AIs should put in place controls[16] so that only customers who choose to use the service will be able to effect such small-value funds transfer transactions.

6.1.2 In any case, AIs should put in place prudent policies and effective safeguards including a proper structure of transaction limits to minimise the risk of unauthorized

[16] For instance, AIs may require customers to apply for or activate, via a secure channel such a service beforehand. Alternatively, small-value funds transfer functions may be disabled or the relevant transaction limit(s) may be pre-set to zero initially.

high-risk funds transfers to unregistered payees. These cover, among others:

(i) funds transfer functions should be disabled or the relevant transaction limit(s) for high-risk funds transfers should be pre-set to zero when a new Internet banking account is first opened. For transaction limit(s) that allow high-value funds transfers to unregistered payees, consideration should be given to resetting the limit(s) to zero if they have not been used for a period of time (such period should not normally exceed 18 months);

(ii) setting the default cross-border fund transfer limit at a level commensurate with the associated risk and allowing customers to lower the limit; and

(iii) consideration should be given to offering the option of dual authorization control for business customers.

6.1.3 Where funds transfer services via Internet banking (or other e-banking channels) allow an AI's customers, on aggregate, to transfer large sums of funds away from the AI to bank accounts (which may or may not be their own accounts) maintained in other institutions within a short period of time, the AI should ensure that its systems and controls for liquidity risk management (including intraday liquidity risk management) remain effective in assessing, monitoring, controlling and managing the increased liquidity risk during both business as usual operations and in any periods of stress.

6.2 Online submission of information

6.2.1 AIs that allow customers to submit information via the Internet (e.g. their corporate websites) should assess the risks and establish appropriate controls, including:

(i) ensuring that adequate encryption mechanisms and other controls are in place to protect the confidentiality and integrity of any sensitive information and documents submitted by the customers;

(ii) implementing system controls to detect and guard against malware attacks through any documents submitted; and

(iii) considering asking the customer to provide supporting documents and conduct additional checks assessed by AIs as appropriate to validate the identity of the customer.

6.3 Account aggregation service

6.3.1 Where an AI intends to offer account aggregation service (AAS [17]) through partnership with other institutions, it should ensure that adequate controls are in place before launching the service. These include controls to ensure that, among others:

(i) the relevant business models are acceptable so as to mitigate the relevant reputation and legal risk involved;

(ii) any applicable local or overseas legal and regulatory requirements including those related to money laundering and terrorist financing have been observed, especially if AIs partner with overseas institutions;

(iii) legal due diligence is performed if AAS involves personal data privacy concerns so as to identify any need for disclosure or obtaining of customer consent. Moreover, appropriate controls should be implemented for customer protection such as when handling any cross-border customer complaints and apportionment of liability for any financial loss of customers that may be caused by fraud cases or system failures involving the partnering institution;

(iv) sufficient security controls are implemented and independent assessment is performed to minimise the risk of intrusion to AIs' systems and

[17] When an AI offers AAS, it generally allows its customers to access their accounts maintained in other institutions (which could be in overseas jurisdictions) through the AI's Internet banking without requiring the customers to separately log in to the Internet banking service of those institutions.

networks through any connections with the partnering institution; and

(v) proper disclosure to customers about the risks and limitations of the service should also be made.

6.4 Provision of other online financial services

6.4.1 As technological and product innovations evolve, AIs may introduce other or new financial services via Internet banking or the Internet. Under Principle 1 of the TCF Charter, the services should be designed to meet the needs of customers. In all cases, AIs should carefully assess the risks (e.g. credit risk, market risk[18], reputation and legal risk) associated with the underlying financial services and how the use of electronic channels (especially if the financial services could be accessible from outside Hong Kong) may have shifted or amplified those risks. Among these risks, AIs should take into account whether their customers are able to transact with them directly using market prices indicated in their Internet banking systems. If so, AIs should review and strengthen corresponding controls where appropriate, including controls to ensure the timeliness and accuracy of the market prices indicated online, even amid periods of unusual market volatility.

6.4.2 If the online financial services offered by an AI involve activities regulated by the Securities and Futures Commission (SFC), AIs should have regard to the relevant regulatory requirements issued by the SFC and the HKMA (see also "SB-1 Supervision of Regulated Activities of SFC-Registered Authorized Institutions") and ensure the requirements can still be fulfilled even if the delivery of the regulated activities involves one or more electronic channels.

7. Security controls in respect of specific e-banking

[18] For instance, market risk may arise if the customers are able to conduct financial transactions through electronic channels with an AI as the counterparty at prices that materially deviate from the prevailing market prices.

channels and payment card transactions

7.1 Internet banking accessed via mobile devices

7.1.1 Apart from the risks generally applicable to Internet banking accessed via personal computers, Internet banking accessed via mobile devices entails certain specific risks such as (i) security vulnerabilities associated with mobile platforms, which may be different from those of personal computers; (ii) the risk of malware or malicious Apps that might potentially capture sensitive customer information, re-direct or conceal notifications or OTPs, or mislead customers into carrying out unauthorized transactions; (iii) the risk of loss or theft of mobile devices; and (iv) customers' security awareness when using mobile devices may be lower than when using personal computers.

7.1.2 As such, AIs should identify and assess the specific risks of the mobile channel (including the relevant mobile platforms) they use and formulate relevant security measures to address these risks, in addition to other controls applicable to Internet banking accessed via personal computers.

7.1.3 Effective customer education programmes tailored for the use of mobile devices should be in place as well as ongoing efforts to identify fake Internet banking Apps, if applicable, and notify customers promptly.

7.1.4 Additional security controls should be implemented for AIs allowing their customers' mobile devices to receive or generate OTPs as the effectiveness of the 2FA may be weakened if the same mobile device is used for (i) accessing Internet banking and (ii) receiving or generating OTPs.

7.2 Banking services accessed via social media platforms or other portals

7.2.1 When banking services can be accessed via social media platforms (including instant messaging services) or other portals, AIs may be exposed to risks such as (i) the risk of leakage of customer data due to insecure

system interfaces or connections between the AIs' systems and those of the platforms/portals; (ii) the risk of unauthorized transactions initiated by fraudsters due to account takeover frauds; (iii) the risk of system intrusion through any direct connections with the systems or security loopholes in the platforms/portals; (iv) reputation risk in any case where there are operational problems caused by the platforms/portals, thereby affecting the AIs' Internet banking; (v) lack of clarity and potential confusion when handling customer disputes which may involve both the usage of Internet banking and the platforms/portals; and (vi) potential cross-border issues if the platforms/portals are subject to laws, regulations or supervisory standards of overseas jurisdictions.

7.2.2 Before partnering with such platforms/portals, AIs should ensure that, among others:

(i) proper assessment of the suitability of partnering with the platforms/portals in the light of relevant factors including the financial conditions and the adequacy of risk management controls and track record of the platforms/portals in guarding against data leakages;

(ii) legal due diligence is undertaken to ascertain that any applicable local or overseas legal or regulatory requirements have been complied with (especially if AIs partner with overseas platforms/portals), including those relating to personal data privacy if customers' personal data would be transmitted to, or stored in, the platforms/portals;

(iii) adequate security controls (e.g. in the areas of network segregation, authentication, confidentiality, integrity, customer data protection, monitoring and malware attacks) are implemented and a rigorous assessment is performed so as to minimise the risk of intrusion into AIs' systems and networks through the connections with the platforms/portals, and the risk of leakage of any customer data transmitted

between the AI and the platforms/portals; and

(iv) appropriate arrangements should be in place for ensuring customer protection such as when dealing with customer complaints and apportionment of liability for any financial loss of customers that may be caused by problems involving the platforms/portals.

7.2.3 For cases where banking services are provided through chat messages via instant messaging applications, appropriate measures should be taken to ensure that proper records are maintained by AIs and customers are properly authenticated before executing the customers' instructions. If such services involve high-risk transactions, the AIs should implement 2FA to authenticate the identity of the customers.

7.3 Self-service terminals

7.3.1 Among the various risks related to self-service terminals, the key operational risks relevant to AIs include:

(i) card skimming attacks;

(ii) fraudsters taking control of the terminals, such as by tampering with the terminals and/or implantation of malware, particularly on terminals using end-of-support software;

(iii) fraudsters compromising the terminals by gaining unauthorized access to the hosts, servers and/or backend systems which connect to the terminals;

(iv) failure to detect and handle counterfeit banknotes for terminals allowing deposits of banknotes; and

(v) disputes with customers caused by possibly confusing system processing of customer

transactions [19] or incidents [20] related to transactions involving banknotes.

7.3.2 AIs should conduct regular assessment to identify and evaluate the relevant risks associated with self-service terminals. Proper risk management measures should be implemented to address the relevant risks. Furthermore, AIs should also closely monitor the emerging cyber attacks and vulnerabilities related to self-service terminals from time to time, and take appropriate measures to address the risks.

7.4 Phone banking

7.4.1 As set out in subsection 4.1.1, AIs should implement adequate customer identity authentication controls in their phone banking operations. When a customer calls in to inquire about the customer's bank account (e.g. balance or transaction history) or perform a transaction via the account, AIs should ensure that effective authentication method is used to verify the identity of the customer. Some commonly used authentication methods include phone banking PIN, biometric authentication and "challenge" questions. In case where only "challenge" questions are used for customer authentication, AI should appreciate that there will be higher customer impersonation risk if the answers to the "challenge" questions are readily available in the public domain or the questions cover only static personal data. AIs should therefore ask a series of more difficult questions, preferably dynamic questions [21] during the customer authentication process. An authentication mechanism that uses different challenge questions between different phone banking authentication sessions, without disclosing all the questions in one session, is considered to be more

[19] For instance, it might be confusing if a customer's account balance will be credited for some time even if no cheque has actually been deposited in a cheque deposit machine.

[20] These include, for instance, (i) when a customer leaves the ATM without taking the banknotes he or she has withdrawn; and (ii) when banknotes are stolen from a customer right after being dispensed from the terminal.

[21] Dynamic questions refer to questions with answers that may change over time and may not be easily guessed by other persons. An example is a question about a customer's recent transaction records.

effective. In addition, adequate controls should be implemented to minimise the risk that AIs' staff (or service providers) who ask the challenge questions and have access to the related answers of a customer would be able to impersonate the customer concerned using the information.

7.5 Contactless mobile payments

7.5.1 Given that payments are provided via contactless channels, contactless mobile payments usually entail certain specific risks such as (i) the risk of leakage of the customer's personal or credit card information through electronic pick-pocketing or eavesdropping in respect of the contactless/wireless traffic between the customer's mobile device and the payee; and (ii) the risk of loss or theft of the customer's mobile device, leading to fraudulent transactions.

7.5.2 In view of the above specific risks associated with contactless mobile payments, AIs should carefully assess the security risks of their proposed service and formulate relevant security measures before launching the service. AIs should also regularly review the effectiveness of these security measures and introduce suitable enhancements as and when appropriate, referencing industry guidance provided by relevant authorities.

7.6 Payment card transactions

7.6.1 Card-Not-Present (CNP) payment card transactions are relatively more susceptible to certain fraud risks compared to card-present transactions due to the absence of the physical card and the opportunity to interact with the cardholder directly for verification during the payment process. Card-issuing AIs should therefore introduce suitable additional measures to manage the risks specific to CNP payment card transactions.

7.6.2 Card-issuing AIs should put in place an effective authentication method for CNP payment card transactions and continue to enhance their

authentication processes to address emerging fraud. Specifically, if 3-D Secure (3DS), a security protocol supporting an additional layer of authentication for CNP payment card transactions, is adopted by merchants, card-issuing AIs should offer an authentication factor that can provide effective protection from the risks of phishing and malware.

7.6.3 Card-issuing AIs should also implement an effective mechanism for monitoring and detecting potentially unauthorized CNP payment card transactions by analysing, for example, data available from 3DS such as IP addresses and cardholders' phone numbers. If suspicious CNP payment card transactions are detected, AIs should obtain additional confirmation from cardholders (e.g. via 2-way SMS or in-App confirmation), even if the transactions have already been authenticated.

7.6.4 Card-issuing AIs should send timely notifications for all CNP payment card transactions (except for recurring payments), or those CNP payment card transactions exceeding a transaction amount threshold if such a threshold has been specified by the relevant customers to the AI concerned. As regards card-present transactions, AIs should adopt a risk-based approach to notifying cardholders of suspicious transactions via effective means.

7.6.5 In addition, card-issuing AIs should notify cardholders of payment card binding with contactless mobile payment services. Moreover, after a payment card is bound to a contactless mobile payment service, AIs should send timely notifications for at least the first three transactions made via the newly bound contactless mobile payment service.

7.6.6 Card-issuing AIs should provide a convenient and effective channel (e.g. hotline or Internet banking) for customers to manage CNP payment card transactions. The channel should allow customers to, among others, (i) enable or disable CNP payment card transactions (except for recurring payments); and (ii) set a limit on CNP payment card transactions (within the overall

credit limits).

8. Fraud and incident management

8.1 Fraud monitoring and remediation

8.1.1 AIs should have a robust and effective automated fraud monitoring mechanism in place to detect, in a timely manner[22], suspicious Internet banking transactions and unusual activities ideally after taking into account their customers' Internet banking usage and behavioural patterns. For e-banking services other than Internet banking, AIs should still implement an appropriate fraud monitoring mechanism that can detect suspicious transactions promptly. AIs should also alert their customers promptly of "High Risk" of fraud based on the information provided by the Police's anti-fraud search engine. In addition, AIs should take appropriate remediation actions to deal with suspicious transactions and unusual activities in a timely manner even after office hours.

8.1.2 AIs should closely monitor trends and developments in emerging fraudulent techniques related to the use of e-banking channels, and regularly enhance or adjust their fraud monitoring systems and remediation process whenever there is a need. During the process, AIs should take into account any fraud intelligence gathered from internal or external sources.

8.1.3 In light of the growing sophistication of deception tactics, AIs should establish dynamic fraud monitoring rules incorporating the latest threat intelligence and customers' historical data and transaction patterns. These rules should encompass a broad spectrum of risk factors, including but not limited to, geographical locations of logins, the time between successive logins and the value of the requested transaction. To bolster fraud detection capabilities, scam intelligence

[22] AIs with Internet banking services that allow real-time transactions after office hours are expected to have the capability of detecting potential frauds on a real-time basis even after office hours.

sources[23] and network analytics tools should be used to promptly identify suspicious transactions and accounts and generate timely alerts to customers.

8.1.4 AIs should assign sufficient designated staff with relevant expertise to promptly handle and respond to the alerts generated by their fraud monitoring mechanism if significant suspicious e-banking transactions or unusual activities are detected during or after office hours. AIs should also ensure that proper procedures and processes are in place for such designated staff to ascertain promptly whether any fraud may actually be being perpetrated via the suspicious transactions or activities identified. These processes may involve suspending the transactions in a timely manner and/or contacting the customers concerned through a reliable channel to verify the transactions or activities. AIs should regularly assess and enhance their capability of fraud monitoring and remediation in light of potential fraud risk amid e-banking development.

8.2 Incident response and periodic drills

8.2.1 Given that the risk of adverse incidents related to e-banking services cannot be completely eliminated, AIs should put in place formal incident response and management procedures for timely reporting and handling of different kinds of incidents (including suspected or actual security breaches, cyber attacks, frauds or service interruptions) affecting their e-banking services both during or outside office hours. The top priority should be to protect the interests of customers who have been or may be affected by the incident.

8.2.2 A communication strategy[24] should be formulated by

[23] Scam intelligence sources may include, among others, threat intelligence provided by fraud experts and data from the Police's anti-fraud search engine "Scameter".

[24] When handling a significant incident affecting a substantial number of customers, the AI concerned is likely to receive a large number of customer and media enquiries. It is therefore essential for the AI concerned to deploy swiftly adequate resources and communication channels (e.g. customer service hotlines) to handle such enquiries.

the senior management to ensure that consistent and up-to-date messages are conveyed to all relevant parties (e.g. customers, media and business partners) on a timely basis. In particular, AIs should proactively notify the customers affected, or likely to be affected, through the most effective means (including considering the possibility of making a press release[25]) and inform them of the key facts relating to the incident and the steps that customers may take[26].

8.2.3 Where the incident involves a disruption of critical e-banking service and may last for a prolonged period of time, AIs should consider making a press release where the situation so warrants, such as when such a press release will be a demonstrable faster or more effective communication means than individual notifications. In particular, an AI is expected to issue a press release (or make a similarly effective notification) shortly after the commencement of any disruption to its critical e-banking service that could affect a significant number of customers if the AI does not have reasonable confidence that the service can be resumed in the near future.

8.2.4 AIs should also formulate, and regularly undertake assessment and practice drills on their incident response and management procedures to ensure sufficient management oversight, adequate capacity and effective incident management capability.

8.2.5 Once an AI becomes aware that a significant incident (including any suspected or confirmed fraud case relating to e-banking) has occurred, the AI concerned should notify the HKMA promptly in accordance with the relevant arrangements set out by the HKMA from time to time.

[25] There could be other relevant factors (e.g. the need to keep the public informed may need to be weighed against the relevant legal considerations, including where appropriate whether a press release may prejudice any ongoing criminal proceedings or any investigation) that the AI should also take into account. The important point is that the actions taken to keep the customers and, where appropriate, the public informed of a significant incident should form an integral part of the incident response and management capability of AIs.

[26] For example, any estimated service resumption time and, where applicable, how customers can protect their interests (e.g. apply for compensation for any losses incurred by the disruption).

9. System availability and business continuity management

9.1 Service level of e-banking for customers

9.1.1 It is important that e-banking services are delivered on a continuous basis with reasonably fast response time, taking into account customers' general expectations. In this connection, AIs should ensure that resilience capability, capacity planning and performance monitoring process of their e-banking systems (particularly for those systems supporting time-critical services such as Internet securities trading services) are commensurate with the scale and nature of their e-banking services.

9.1.2 AIs should ensure that their controls relating to system resilience and their capacity planning for e-banking cover all related systems and infrastructure components within their institutions as well as those of any relevant service providers to ensure stability, performance and continued system availability of e-banking to the relevant customers.

9.2 Capacity planning

9.2.1 A thorough review of the system capacity of the relevant systems and infrastructure should be conducted from time to time to identify any potential weaknesses that may affect the stability and performance of e-banking. Regular capacity planning and performance reports should be produced for senior management's attention. Any necessary enhancement measures to rectify the identified weaknesses should also be implemented promptly to avoid possible system instability.

9.2.2 Guidelines for capacity planning should be established, which clearly set out, among others, system utilization threshold and corresponding precautionary measures (e.g. to step up monitoring of system utilization and perform system upgrades when the peak utilization level reaches the predetermined capacity levels). A capacity planning methodology should also be developed to help estimate future capacity

requirements (taking into account the trend analysis of system utilization, projection of customer growth and transaction volume, progress of system capacity upgrades, system performance issues encountered, etc.) and turn business requirements into IT capacity plans. The methodology should take into account capacity implications of any new business initiatives and, anticipated growth of the utilization of the relevant e-banking services. In particular, for time-critical e-banking such as Internet securities trading services, the capacity plan should take into account the possibility of a sudden upsurge in transactions during particular timing or situations.

9.2.3 It may be prudent that a fast-track software and hardware procurement process is formulated, which includes making prior arrangement with the related software and hardware providers to allow upgrading of system capacity within a short period of time when such a need arises. In any case, adequate end-to-end system stress testing should be conducted with adequate coverage of all relevant systems and infrastructure components to identify potential performance bottlenecks in advance.

9.3 Performance monitoring

9.3.1 Regardless of the scale of e-banking, an automated performance monitoring and alert system, which covers all critical systems and infrastructure components supporting e-banking, should be in place so that any potential system interruption or performance degradation both during or after office hours could be detected and handled by designated staff in a timely manner.

9.4 System resilience

9.4.1 AIs should ensure that there is no single point of failure in the systems/infrastructure components nor unnecessary connections or dependency upon less critical systems. It is important that the actual effectiveness of the resilience of the system should be properly verified and tested.

9.4.2 If the system resilience of AIs depends on the cooperation of external service providers, they should maintain an adequate level of monitoring of the system resilience of these service providers and understand their contingency planning arrangements. If the service providers concerned are AIs' outsourcing agents, AIs should assess the system resilience controls of the service providers as part of the assessment of their own system resilience.

9.5 Controls for coping with system disruptions

9.5.1 AIs' IT function should establish a service level agreement with business lines covering availability of e-banking systems. Against this system availability benchmark, AIs should maintain and service the relevant IT facilities and equipment in accordance with industry practices and suppliers' recommended service intervals and specifications. Moreover, AIs should formulate and undertake regular practice drills to test the relevant IT disaster recovery plan and procedures to ensure that their e-banking services can be resumed within a short period of time and in accordance with the AIs' business recovery requirements, taking into account the duration required for trouble-shooting, problem fixing and switching over to the back-up e-banking systems if needed.

9.5.2 AIs should take appropriate measures having regard to common issues that could lead to disruptions of e-banking. Moreover, AIs should implement proper precautionary measures before and during scheduled maintenance or drills (see Annex B for examples of precautionary measures).

9.5.3 Moreover, AIs should implement adequate controls to promptly detect and respond to the threats posed by distributed denial-of-service (DDoS) or other cyber attacks that could directly or indirectly cause disruptions to e-banking systems. These controls should be validated (e.g. testing at point of service activation or a production-like system environment) and periodically reviewed to ensure their ongoing effectiveness against any emerging techniques in

DDoS attacks.

9.5.4 AIs should implement sufficient and effective alternative service delivery channels to ensure e-banking services can be provided continuously to customers as far as appropriate. In particular, if an Internet banking system is temporarily not accessible, AIs should ensure that their other service channels will have the capacity and related operational procedures to provide an acceptable level of service to their customers, taking into account the anticipated customers expectation, in relation to critical functions (e.g. funds transfers, securities trading)..

———————————

Contents	Glossary	Home	Introduction

Annex A: Items to be reported in independent assessment

A.1 In general, a report of independent assessment should cover at least the following items:

A.2 Period of assessment

A.2.1 The report should state when (a particular snapshot or a period of time) and at what stage of the preparation for the launch or major enhancement of e-banking service (e.g. design stage or testing stage of the e-banking system) the independent assessment was conducted.

A.3 Scope & approach

A.3.1 The report should describe the scope of, and approach adopted in, the assessment. In particular, the scope should mention the applicable subsections of this module and other applicable HKMA and industry guidelines and circulars that are relevant to the underlying financial services and the electronic delivery channel concerned, and the reasons for any material exclusion of applicable guidance. Furthermore, the report should set out what controls and system components, as well as what portion of the AI's internal networks and network equipment were covered in the independent assessment, against the scope as identified above.

A.3.2 The assessor should perform more thorough review and verification as appropriate on areas of higher risk. For AIs offering e-banking services of higher risk such as Internet banking and any financial services delivered using emerging technologies, they should consider including in their independent assessment penetration tests.

A.4 Summary of assessment results

A.4.1 The report should include the following information:

- findings identified in the assessment, including any serious deficiencies identified during the course of the assessment even if such issues have been rectified before the report is issued. There should also be explanations of the risk implication of the findings, and the assessor's assessment of the level of risk associated with the findings;

- recommendations of the assessor to assist in addressing the findings; and

- management response to the findings and recommendations, including the actions taken or to be taken to address the findings, the target date for completing the actions, and any interim measures taken or to be taken (the management response may be included in a separate report).

A.4.2 If the management adopt alternative methods to address the weaknesses identified by the assessor or if the assessment discloses material weaknesses, the AI normally needs to request the assessor or another independent expert to perform a follow-up review of the matters concerned.

Annex B: Examples of precautionary measures before and during scheduled system maintenance or drills

B.1 Management oversight and monitoring over the scheduled system maintenance/drills and related preparation/follow-up actions;

B.2 Proper preparation (e.g. proper maintenance/recovery procedures, testing of the changes with satisfactory results, well-tested fall-back procedures to cater for any exceptional and unexpected situations) before the maintenance/drills;

B.3 Live test after the scheduled system maintenance/drills to ensure the effective operation of the relevant services;

B.4 Adequate advance notifications to relevant customers about the service outage (e.g. the services that would be affected and the duration of the impact);

B.5 Arrangements that ensure prompt responses to customer and media enquiries that may arise during or after the affected period; and

B.6 Procedures for proper and timely escalation to senior management and public communication plans to cater for exceptional and unexpected situations (e.g. the scheduled system maintenance/drills cannot be completed in time and the services cannot be resumed as scheduled).