澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

Circular No. 005/B/2023-DSB/AMCM
(Date: 26/06/2023)

Guideline on Risk Management of Electronic Banking

The Monetary Authority of Macao (AMCM), under the powers conferred by Article 9 of the Charter approved by Decree-Law No.14/96/M of 11th March and by Article 6 of the Financial System Act of Macao approved by Decree-Law No. 32/93/M of 5th July, establishes the following:

1 INTRODUCTION

1.1 Developments and innovations in technologies are transforming the way in which authorized institutions operate, and have been enabling them to deliver their services and products to customers on either private or public network, through electronic, interactive communication channels such as the internet (e.g. web, mobile), interactive terminals, fixed telephone network or other electronic terminals/devices. For the purpose of this Guideline, electronic banking typically refers to financial products and services[1] provided to customers via internet banking[2], self-service terminals[3], and phone banking[4] channels.

1.2 While electronic banking brings benefits, it also carries risks. It is therefore necessary for authorized institutions to implement risk management controls that are commensurate with the risks associated with the types, complexity and amounts of transactions allowed and the electronic channels adopted by them.

---

1 Financial products and services include but not limited to the followings: applying new products and services, viewing loan and deposit-account balances and transactions, performing transactions of electronic banking (include e-wallets and prepaid cards), transferring funds between accounts, purchasing stocks and investment products, submitting information, viewing or managing aggregation account, making retail payment via mobile banking application, the placing and using of funds on e-wallets or prepaid cards, gaining access to self-service terminal, and gaining access to third party payment platform for providing electronic payment service etc.

2 Internet banking refers to the provision of financial services via internet to customer's devices (including personal computers and mobile devices).

3 Self-service terminal refers to interactive terminals (including but not limited to automatic teller machines (ATMs), cash deposit machines (CDMs), cheque deposit machines and virtual teller machines) used by authorized institutions to provide financial services to their customers.

4 Phone banking refers to the provision of financial services via telephone line or mobile telecommunication network (including manned and Interactive Voice Response (IVR) phone banking service). For the purpose of this Guideline, phone banking does not include the provision of banking services for the purpose of sales promotion, activity notification/call-back confirmation, or customer relationship management.

1.3 The aim of this Guideline is to set forth the key principles and provide guidance for authorized institutions to identify, assess and manage the risks associated with electronic banking from both technology and operation perspectives.

1.4 This Guideline applies to either locally incorporated authorized credit institutions or branches of overseas banks in Macao. All such credit institutions that are engaging or going to engage in electronic banking activities are expected to adopt the key principles of the Guideline which will assist them in establishing a sound and robust risk management process, strengthening the system availability, security, and recovery capability, and deploying strong cryptography and key management practices to protect customer data. Where applicable, this Guideline would also apply to the following institutions[5] that adopt/will adopt the use of electronic communication channels in the delivery of their services:

(a) finance companies licensed under Decree-law no. 15/83/M;

(b) institutions licensed under Decree-Law no. 25/99/M to carry out assets management activities;

(c) investment fund management companies licensed under Decree-Law no. 83/99/M; and

(d) financial intermediaries and other financial institutions licensed under the Financial System Act.

1.5 The risk management challenges to authorized institutions, the key risk management processes that are expected of them and the supervisory requirements for authorized institutions to conduct relevant assessments on their electronic banking systems are given at the ensuing paragraphs. It should be noted that the recommendations contained in this Guideline should not be considered definitive, since technologies continue to evolve rapidly. Authorized institutions should always take into account the other relevant and applicable industrial standards and practices to ensure that their risk management processes for electronic banking are both current and appropriate.

1.6 The AMCM endorses the risk management principles and sound practices outlined in the Basel Committee on Banking Supervision's (the Basel Committee) papers "Risk Management Principles for Electronic Banking" (http://www.bis.org/publ/bcbs98.htm) and the "Management and Supervision of Cross-Border Electronic Banking Activities" (http:/www.bis.org/publ/bcbs99.htm) issued in July 2003. Authorized institutions are encouraged to also read and understand the main principles of these documents.

[5] Credit institutions and the institutions mentioned herein are collectively referred to as "authorized institutions".

2 RISK MANAGEMENT CHALLENGES POSED BY AND RISK ASSOCIATED WITH ELECTRONIC BANKING

2.1 As identified by the Basel Committee, the fundamental characteristics of electronic banking pose a number of risk management challenges for banking institutions:

Firstly, the unprecedented speed of change relating to technological and customer service innovation exert competitive pressures for institutions to roll out new business applications on very compressed time frames. Competition also intensifies the need to ensure that adequate strategic assessment, risk analysis and security reviews are conducted prior to implementing new electronic banking applications.

Secondly, the integration of transactional electronic banking websites and associated retail and wholesale business applications with legacy computer systems increases the institutions' dependence on sound system design and architecture as well as system interoperability and operational scalability.

Thirdly, the increasing dependence on information technologies increases and furthers a trend towards more partnership alliances and outsourcing arrangements with third parties, many of whom are unregulated.

Fourthly, the ubiquitous and global nature of open electronic networks magnifies the importance of security controls, customer authentication techniques, data protection, audit trail procedures, and customer privacy standards.

2.2 Although the types of risks generated by electronic banking are not new, the different ways in which some of the risks arise, and their magnitude and possible consequences, take on new dimensions. From a supervisory perspective and for the purpose of banking supervision, the AMCM has identified the following categories of risk that are mostly associated with electronic banking. Familiarization with these risks will help authorized institutions to identify, measure, monitor, and control them:

(a) Strategic Risk. This refers to the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. Management should understand the risk associated with electronic banking before deciding to develop a particular class of electronic banking products. Before introducing an electronic banking product, management should consider whether the product and technology are consistent with the authorized institution's strategic plan and whether adequate expertise and resources are available to identify, monitor, and control risk.

(b) Operational Risk. This is the risk of error or fraud or the risk that systems will fail to adequately record, monitor, and account for transactions or positions. A high level of operational risk may exist with electronic banking if the business lines are not carefully planned, implemented, and monitored. Authorized

institutions that offer electronic banking products must be able to meet their customers' expectations and also ensure that they have the right product mix and capacity to deliver accurate, timely, and reliable services. Customers who do business through electronic means are likely to have little tolerance for errors or omissions. Attacks or intrusion attempts on authorized institutions' computer and network systems are a major concern and authorized institutions should have sound preventive and detective controls to protect their electronic banking systems from cyber-attacks. Contingency and business resumption planning is also necessary for authorized institutions to be sure that they can deliver electronic banking products and services in the event of adverse circumstances.

(c) Legal Risk. The risk to earnings or capital arises from violation of or non-conformance with laws, rules, regulations, or ethical standards. Legal risk exposes an authorized institution to fines, payment of damages, and the voiding of contracts and can lead to a damaged reputation, limited business opportunities and reduced expansion potential. While most electronic banking customers will continue to use both non-electronic (e.g. physical branches) and electronic banking delivery channels, authorized institutions should ensure that all such delivery channels will transmit a consistent and accurate message to customers and comply with the laws, rules and regulations.

(d) Reputational Risk. The current and prospective impact on earnings and capital arises from negative public opinion. An authorized institution's reputation can be damaged by electronic banking services that are poorly executed or otherwise alienate customers and the public. Well-designed marketing, including disclosures, is one way to educate potential customers and help limit reputational risk. Authorized institutions must make sure that their customers understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using the system. An authorized institution's marketing program must present the product fairly and accurately.

(e) Liquidity Risk. The risk to the earnings or capital arises from the operational impact due to the inability to provide adequate funds to cover redemption and settlement demands in a timely manner. Funding liquidity risk may be significant for authorized institutions that offer electronic banking as they may allow customers to transfer large amounts of money to other institutions more easily when compared with the traditional way of banking. Authorized institutions should pay attention and put in place appropriate liquidity risk management policies and procedures prior to executing the high-value or high volume transactions that exceed pre-defined liquidity risk tolerance levels. Additional sound practices for managing liquidity risk can also be found in the AMCM's "Guideline on Management of Liquidity Risk".

(f) Credit Risk. The impact on viability and profitability of authorized institutions arises from borrower's inability to settle an obligation for full value either when due or at any time thereafter. Regardless of the service delivery channel,

authorized institutions should have adequate procedures to assess the credit application and evaluate borrowers' credit worthiness, in order to properly manage the relevant credit risks.

3 BOARD AND MANAGEMENT OVERSIGHT

3.1 The board of directors and senior management have the responsibility and accountability to manage and control the risks associated with electronic banking. A sound and robust risk management for electronic banking allows them to fully recognize the challenges posed by the fundamental characteristics of electronic banking and to possess the knowledge and skill to manage the authorized institution's use of electronic banking technologies and products, thereby appropriately modifying the existing control system to ensure that it is robust enough to identify, assess, monitor and control the risks associated with electronic banking. For this reason, amongst others, the board and/or senior management should:

(a) conduct adequate up-front strategic review and thorough analysis of the costs, benefits, and risks before:

- reaching decision to integrate electronic banking activities into the corporate strategic goals;
- establishing the authorized institution's risk appetite; and
- determining the level of complexity of the electronic banking services offered and the technologies supporting such services.

(b) assess the feasibility of the business plans and ascertain that the authorized institution has sufficient financial, human and technical resources and expertise (which may include in-house expertise or those acquired from third parties) as well as adequate risk management and internal control procedures to provide electronic banking services;

(c) establish policies and procedures that are "fit for purpose" to assess, monitor and control the risks associated with electronic banking in a timely manner. These include the establishment of:

- key delegations and reporting mechanisms including the necessary escalation procedures for incidents that impact the authorized institution's safety, soundness or reputation;
- where applicable, control measures to ensure compliance with the due diligence requirements for non-face-to-face customers stipulated in relevant supervisory guidelines (e.g. the AMCM's "Anti-Money Laundering and Combating the Financing of Terrorism Guideline for Financial Institutions" and relevant industry guidance); and

- other necessary steps to address the unique risk factors associated with ensuring the integrity and availability of electronic banking products and services.

(d) maintain a strong security control system for electronic banking related activities, in order to manage and minimize security risks posed by potential internal and external security threats (see also paragraph 4);

(e) establish monitoring mechanism, process and procedure to effectively detect and respond to suspicious and abnormal transactions or activities (see also paragraph 5);

(f) establish effective business continuity management controls to manage unexpected adverse events impacting service availability, which include business continuity and contingency plan, incident response plan for handling internal and external risks, and necessary notification upon service disruption (see also paragraph 6);

(g) establish a comprehensive and ongoing due diligence and oversight process for managing authorized institution's outsourcing relationships and other third-party dependencies supporting electronic banking (see also paragraph 7); and

(h) establish effective management controls for its cross-border electronic banking activities, if any (see also paragraph 8).

3.2 In view of the constant changes occurring in the electronic banking environment, the board and senior management should review the relevant policies and procedures on a regular basis to ascertain that they are both appropriate and timely to the nature and scope of electronic banking activities. The board and senior management should assess the financial impact of the implementation and ongoing maintenance of electronic banking services and consider the potential impact on authorized institution's customer base, loan quality and composition, deposit volume, volatility, liquidity sources, and transaction volume, as well as the impact on other relevant factors that may be affected by the adoption of new delivery channels. These areas should be monitored and analyzed on an ongoing basis to ensure that any impact on authorized institution's financial condition and risk profile arising from electronic banking services is appropriately managed and controlled.

3.3 The board and senior management's monitoring responsibility of electronic banking activities may also be exercised through the review of periodic reports tracking customer usage, complaints, downtime, unreconciled transactions, and system usage relative to capacity. An appropriate independent audit function is also an important component of monitoring. The audit coverage should be expanded commensurate with the increased complexity and risks inherent in electronic banking activities and should include the entire applicable electronic banking processes such as network configuration and security, interfaces to legacy systems, regulatory compliance, internal controls, support activities performed by third-party providers, etc.

4 SECURITY CONTROLS

Internet Banking

4.1 Authorized institutions should recognize that internet banking must be secure to achieve a high level of confidence with both customers and businesses. It is the responsibility of bank management to provide adequate assurance that transactions and information processed through electronic delivery channels are properly protected. For this reason, a strong and comprehensive internet banking security control system should be maintained.

4.2 To address and control the relevant risks and security threats in internet banking, the security control system of authorized institutions should meet the following objectives:

(a) **Authentication.** Authorized institutions should use reliable and appropriate authentication methods to validate and verify the identity and authorization of their internet banking customers. The authentication method an authorized institution chooses to use in a specific internet banking application should be appropriate and reasonable considering management's risk assessment of the applications/transactions being used/processed. Authorized institutions should weigh the cost of the authentication method, including technology and procedures, against the level of protection they afford and the value or sensitivity of the transaction or data to both the institutions and the customers. Authorized institutions should also note that the constituents of a reasonable system might change over time as technology and standards evolve.

In basic terms, the process of authentication is to validate the claimed identity of the customer by verifying one or more of the three factors of "what the customer knows" (usually a password or personal identification number), "what the customer has" (such as a smart card, a security token or digital certificate) and "what the customer is" (such as a biometric characteristic like a fingerprint/iris pattern/facial image).

Authentication methods that depend on more than one factor are typically more difficult to compromise than a single-factor system[6] and would thereby have a higher level of reliability. Therefore, two-factor authentication ("2FA", e.g. requiring the customer to conduct another factor such as a one-time password

[6] The use of a customer identification and password are considered single-factor authentication since both items are something the customer knows.

(OTP)[7], transaction signing[8] or biometric authentication) should be required for electronic banking channels that allow high-risk transactions[9, 10]. For internet banking, authorized institutions should consider implementing 2FA at login to validate customers' identities. In addition, authorized institutions should implement 2FA to re-authenticate a customer's identity before performing each high-risk transaction. However, merely for trade execution and subscription of financial products with frequent price movements, authorized institutions may choose to require 2FA just once to authenticate customers' identities for each login session before performing such high-risk transactions, rather than 2FA for each transaction.

It is also important that the authentication methods adopted for internet banking services are assessed and evaluated on a continuous basis to ensure the authentication mechanism remains effective. Common practices used to maintain the effectiveness of authentication mechanisms for verifying customers' identities include:

- risk assessments over authentication methods are conducted (i) prior to adoption, (ii) periodically after implementation, and (iii) when triggered by significant incidents which impact the overall security posture of the specific authentication methods adopted;
- a reasonably short validity period[11] is implemented over OTP such that the OTP cannot be used for authentication upon expiry of the specified duration;
- sufficient customer identity verification is performed in a secure manner (e.g. with proper procedure to validate the identity with appropriate 2FA and security question) when changes occur to the existing authentication factors (e.g. password, authentication tokens, biometric data recorded on the electronic device such as fingerprint/ iris patterns/ facial images). Timely

7 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.

8 Issued by authorized institutions to verify the authenticity by creating one-time confirmation code through pre-registered channels (e.g. digital signatures).

9 High-risk transactions should at least cover high-risk funds transfers which include (i) funds transferred to unregistered third party payees; (ii) bill payments made to unregistered high-risk merchants; and (iii) online transfers of customers' monetary or non-monetary benefits or interests (e.g. credit card rewards points) to unregistered third parties.

10 Apart from the afore-mentioned high-risk funds transfers, high-risk transactions also include (i) online registration of third party payees or high-risk merchants, (ii) creation of new account linkages (e.g. binding banking account with a social media account for receiving important information or binding a customer's bank account or payment card with mobile payment application), (iii) upward revision of transaction limit(s), (iv) changes of account contact details (e.g. email address, contact phone number, postal address), (v) disclosure of the full contact details of a customer's account on the internet banking application screen, (vi) administrative functions on banking accounts (e.g. user account creation), (vii) trade execution and subscription of financial products.

11 In general, the validation period of OTPs should not exceed 100 seconds.

notification should be sent to customers via different channels upon changes in sensitive information used for authentication;

- cryptographic measures and system integrity controls are implemented to protect sensitive data used for authentication; and
- session controls are implemented to block concurrent sessions and terminate login sessions after a period of inactivity to prevent attacks on authenticated sessions (e.g. session hijacking).

(b) **Non-repudiation.** Non-repudiation involves creating proof of the origin or delivery of electronic information to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent. Authorized institutions should, commensurate with the materiality and type of the internet banking transaction, implement adequate measures to safeguard the accuracy and completeness of electronic information transmitted over external and internal networks to help establish non-repudiation and ensure confidentiality and integrity of internet banking transactions. For example, the use of public key cryptography, digital signature and digital certificate arrangements can uniquely identify the person who initiates a transaction, append a digital signature to the transaction, detect unauthorized modifications and prevent subsequent disavowal.

(c) **Data and transaction integrity.** Data integrity refers to the assurance that information transmitted, processed or stored is not altered without authorization. Failure to maintain the data integrity of transactions, records and information can expose authorized institutions to financial losses as well as substantial legal and reputational risks. Authorized institutions should therefore ensure that appropriate measures are in place to ascertain the accuracy, completeness and reliability of information processed, transmitted, or stored. The common practices used to maintain data integrity within an internet banking environment include:

- internet banking transactions should be conducted in a manner that makes them highly resistant to tampering throughout the entire process;
- internet banking records should be stored, accessed and modified in a manner that makes them highly resistant to tampering;
- internet banking transaction and record-keeping processes should be designed in a manner to make it virtually impossible to circumvent detection of unauthorized changes;
- adequate change control policies, including monitoring and testing procedures, should be in place to protect against any internet banking system changes that may erroneously or unintentionally compromise controls or data reliability; and

- any tampering with internet banking transactions or records should be detected by transaction processing, monitoring and record keeping functions.

(d) **Segregation of duties.** Segregation of duties is an essential element of internal controls designed to reduce the risk of fraud in operational processes and systems, and to ensure that transactions and assets are properly authorized. Responsibilities and duties that should be separated and performed by different personnels include operating systems function, system design and development, application maintenance programming, computer operations, database administration, security administration, data security, librarian and backup data file custody. It is also desirable for job rotation and cross training for security administration functions to be instituted. Transaction processes should be designed so that no single person could initiate, approve, execute and enter transactions into a system in a manner that would enable fraudulent actions to be perpetrated and concealed.

(e) **Authorization controls.** Authorized institutions need to strictly control authorization and access privileges, as failure to provide adequate authorization control could allow individuals to alter their authority, circumvent segregation and gain access to internet banking systems, networks, databases or applications to which they are not privileged. Authorization and access rights should base on job responsibility and the necessity to have them to fulfil one's duties. In principle:

- users should be granted access rights on a need-to-use basis. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorization should be allowed to access confidential information and use system resources and is solely for legitimate purposes; and
- proper measures should be in place to ensure access rights that are no longer needed should be revoked or disabled promptly.

(f) **Maintenance of audit trails.** An authorized institution's internal control may be weakened if it is unable to maintain clear audit trails for its internet banking activities. Authorized institutions should therefore ensure that clear audit trails exist for all internet banking transactions so that all critical internet banking events and applications can be independently audited. In particular, clear audit trails should exist under the following types of internet banking transactions:

- the opening, modification or closing of a customer's account[12];
- any transaction with financial consequences;
- any authorization granted to a customer to exceed a limit; and
- any granting, modification or revocation of systems access right or privileges.

(g) **Confidentiality of sensitive information.** Confidentiality is the assurance that sensitive information is only accessible by authorized parties. Misuse or unauthorized disclosure of sensitive data and records exposes an authorized institution to both reputational and legal risks. Therefore, authorized institutions should implement appropriate technologies, such as cryptographic technologies, to maintain confidentiality and integrity of sensitive information while it is being transmitted over the internal and external networks and when they are stored inside the authorized institutions' internal systems. Authorized institutions should adopt secure and internationally-recognized cryptographic algorithms, where the strengths of the algorithms have been subjected to extensive tests, to protect the customer information over the external networks including the internet, and highly sensitive information such as customer login credentials which are kept in storage and transited over internal networks.

4.3 The security controls of authorized institutions may involve the use of hardware and software tools and other security measures to deter unauthorized access to all critical internet banking systems, servers, networks, databases and applications. In addition to the fulfilment of the objectives to safeguard the authenticity and confidentiality of data and operating processes as discussed in paragraph 4.2 above, authorized institutions should ensure an appropriate level of application security, establish infrastructure that conforms to industry sound practices and implement other sufficient controls to manage the unique security risks confronting them. The relevant control considerations include but not limited to:

(a) ongoing awareness of attack sources, scenarios, and techniques;

(b) secure network infrastructure with the design of the demilitarized zone (DMZ) and multi-tiered firewalls;

(c) up-to-date equipment inventories and network maps;

(d) rapid identification and mitigation of vulnerabilities;

(e) network access controls over external connections;

(f) use of intrusion detection tools and relevant response procedures; and

[12] Authorized institutions should have applied a robust customer identification, verification and due diligence process at the outset of its relationship with customers, in accordance with the AMCM's "AML/CFT Guideline for Financial Institutions" and relevant industry guidance.

(g) physical security of all internet banking computer equipment and media.

4.4 Authorized institutions should conduct technical security assessments to validate the effectiveness of security controls before deployment of any significant changes or major enhancements[13] to the internet banking systems. In addition, technical security assessments should be conducted on the existing internet banking systems (i.e. without any significant changes being introduced) on a regular basis (e.g. at least annually for vulnerability scanning and penetration test) to assess the continued effectiveness of security controls. The relevant technical security assessments should include, but not limited to:

(a) **Configuration review.** Authorized institutions should perform configuration review over the network components such as firewall, servers and any other relevant devices supporting the internet banking system to reduce the security risk by restricting unauthorized activities at the network components and condensing the attack surface;

(b) **Source code review.** Authorized institutions should perform source code review for any code changes, especially before launching significant changes or major enhancements on internet banking system, to identify security defects arising from coding error, insecure coding practices or malicious attempts. The scope, approach and outcome of source code review should be formally documented. For internet banking systems that are developed and/or maintained by third party service provider(s), authorized institutions should require its service provider(s) to provide independent assessment reports and/or relevant evidence to show that source code review has been performed. Such assessment results should be reviewed by authorized institutions;

(c) **Vulnerability scanning.** Authorized institutions should perform vulnerability scanning regularly on the external and internal network components that support the internet banking system to identify security vulnerabilities and related potential risks. Remediation measures (e.g. patching) should be applied to fix the identified security vulnerabilities in a timely manner after assessing the possible impact and risk level; and

(d) **Penetration test.** Penetration test should be performed in a risk-based approach by qualified independent party regularly and after major changes to the system architecture or asset, simulating the actual attack scenario to cover all the components that supports internet banking system to identify vulnerabilities and potential threats.

4.5 Authorized institutions should evaluate their security control system periodically to ensure continued effectiveness. Ongoing training at different levels of staff should also

[13] Significant changes or major enhancements refer to changes of system infrastructure or functions, which do not include any maintenance work or daily/routine operational tasks such as patching, hardware replacement, etc.

be provided in order to equip them with the necessary skills to comply with the security control system and to keep abreast of the technological and industrial advancements. For those who oversee the key technology controls such as network security, virtualization security, database security and endpoint security, technical training is particularly important.

4.6 With the increasing use of internet banking, the online services to customers are expanding. Authorized institutions should recognize certain risks adhering to specific internet banking services and implement adequate controls to minimize those risks. For this reason, amongst others, authorized institutions should implement additional security measures given under paragraphs 4.7 to 4.12 below to address the risks of **Funds Transfers, Online Submission of Information, Remote On-boarding Service, Account Aggregation Services**[14] and **Open Application Programming Interface** if such internet banking services are provided.

4.7 To ensure sufficient security controls are implemented for **Funds Transfers**, authorized institutions should implement appropriate authentication measures before conducting a high-risk funds transfer as given under paragraph 4.2(a). Nonetheless, authorized institutions have the flexibility to waive the 2FA requirement for the small-value funds transfers to unregistered payees if the amount does not exceed the transaction limit set by customers and authorized institutions. The transaction limit defined by customers should be bounded by the limit determined by the authorized institutions. Amongst others, the authorized institution should:

(a) put in place prudent policies and effective safeguards including setting up the proper structure of transaction limits to minimize the risk of unauthorized high-value funds transfers to unregistered payees. Authorized institution should disable high-risk funds transfer functions or preset the relevant transaction limits to zero when the new internet banking account is first created. In addition, transaction limits that allow high-value funds transfer to unregistered payees should be considered resetting to zero if the account has not been used for a period of time (such period should not normally exceed 18 months);

(b) implement appropriate controls to prevent customers from unknowingly using the small-value funds transfer function such as requiring the customer to apply for or activate the service beforehand in order to use the small-value funds transfer function. In any case, timely notification should be sent to the customers through the pre-registered channel(s) once the customers initiate the funds transfer;

(c) clearly inform customers about the risk implications when activating the funds transfer functions, setting or increasing the limits;

[14] Account aggregation services refer to the service that compiles information from different institutions into one place, which allow customers to access their account information of other institutions without logging in to those institutions separately.

(d) offer the option of dual authorization control for corporate customers; and

(e) ensure the liquidity risk management systems are capable to monitor, assess, control and manage liquidity risk effectively under both normal and stressed conditions, especially when large amounts of funds are transferred out from the authorized institution within a short period of time through internet banking channels.

4.8 Sufficient security controls should be implemented to minimize the risks arising from the **Online Submission of Information** service where customers can submit their information and documents via internet. Authorized institutions should establish appropriate system measures considering the data sensitivity and common attack vectors. Among others, authorized institutions should:

(a) deploy advanced cryptographic mechanisms and other protective controls to uphold the confidentiality and integrity of the sensitive information and documents submitted by the customers;

(b) implement adequate protective controls on internet banking systems against malware attacks through any documents submitted;

(c) establish monitoring systems to detect and respond to malicious documents uploaded, and;

(d) perform additional checks to verify the customer's identity.

4.9 Authorized institutions should adopt appropriate and effective process and technologies for **Remote On-boarding Services**[15] to control the impersonation risks, money laundering and terrorist financing (ML/TF) risks. When customers are not physically present for identification purposes, it is harder for authorized institutions to verify the authenticity of the documents and the identity of the customers. Authorized institutions should:

(a) properly validate the identity information such as checking the security features of the submitted identity documents and extracting identity information using reliable and independent technology (such as optical character recognition). Such extracted identity information should be compared with the customer's live biometric data obtained using the appropriate and effective processes and technologies (e.g. facial recognition, fingerprint, iris scans, liveness detection or real-time video conference);

(b) appropriately maintained the relevant documents and information of the customers involved in the remote on-boarded process and ensure they can be timely retrieved upon request;

[15] Authorized institutions should adopt the additional controls as outlined in the AMCM's "Industry Guidance on AML/CFT Controls – Remote On-boarding of Customers", as necessary.

(c) assess any new technologies prior to adoption for remote on-boarding service and monitor the effectiveness of the technologies on an ongoing basis, especially during the early stages of implementation and operation.

4.10 Authorized institutions should deploy appropriate controls prior to the launch of **Account Aggregation Service** through partnership with other institutions. In particular, authorized institutions should:

a) review the scope of service against applicable local or overseas legal and regulatory requirements, including but not limited to personal data privacy, money laundering and terrorist financing requirements;

b) assess the business model and implement appropriate measures to address potential risks (e.g. reputational risk, legal and compliance risk, operational risk) arise from the service;

c) establish appropriate procedures in handling customer enquiries or complaints and any financial dispute with partnering institutions;

d) implement network and application security controls to minimize the risk of intrusion on internet banking systems through any connections with the partnering institutions; and

e) obtain customer prior consents and provide sufficient disclosure to customers about the terms and conditions, risks and limitations of the service.

4.11 Application Programming Interface (API) refers to the interface between different software applications and enables communication between applications for data transmission or function calls. **Open APIs** are APIs opened by an organization that allows third party (e.g. customers, business partners[16]) to access its information systems.

In general, Open API can be classified into transactional and informational APIs which facilitate different internet banking services (e.g. account information inquiry, fund transfer, trade execution) provided by the authorized institutions.

As additional security risks may arise from allowing Open API to the public, authorized institutions should consider implementing additional security measures with reference to the nature, complexity and criticality of the Open API functions. In particular, authorized institutions should:

a) conduct sufficient functional, performance and security tests before deploying any new Open API service into the production environment;

[16] Include financial institutions.

b) maintain formal documentations and records on any changes of Open API specifications;

c) conduct comprehensive due diligence on its business partners who support the delivery of Open API services[17] that involve sensitive customer information and high-risk transactions. Authorized institutions should publish a list of business partners and their relevant products (such as the mobile applications or websites) via their official channels to ensure public trust and consumer protection;

d) obtain customers prior consent and provide sufficient disclosure to customers about the terms and conditions and risks before sharing any customer data to business partners; and

e) establish a risk-based ongoing monitoring mechanism to continuously review the system architecture, security and data standards to ensure that the Open APIs in use continue to fulfil relevant regulatory requirements and industry best practices.

4.12 **Mobile Banking (including mobile payment)** is becoming an important platform to provide financial services. Specific risks are associated with mobile banking platform, which include but not limited to the poor authentication of mobile customers, mobile malware and viruses, insecure data transmission and storage on the mobile device. For this reason, among the security measures generally applicable to internet banking, authorized institutions should:

a) implement strong authentication controls on mobile banking. As the effectiveness of 2FA may be weakened if using the same mobile device to access internet banking and receive or generate OTP, authorized institutions should implement additional risk mitigating measures. For example, the change of customer's mobile phone number should be permitted only through secure channels with adequate identity validation (other than 2FA via SMS OTP), and high-risk transactions should only become effective after a reasonably long delay, with consideration of the relevant risks of the transactions and authorized institution's authentication mechanism and fraud monitoring capability. Additional measures to strengthen the authentication control on OTP, such as limiting the period of validity of OTP, implementing sound cryptographic key management practices, and conducting regular assessments on the effectiveness of OTP adopted for customer authentication, should also be implemented;

b) put effective security controls in place to protect data processed and stored on customers' mobile devices. Authorized institutions should ensure that sensitive customer data are not stored or cached in the mobile devices after termination of the mobile banking session whenever practicable;

[17] The services including but not limited to (i) online submission/application for credit card, loans or other products or services; (ii) retrieval and alternation of the account information by customer; (iii) initiation of transactions, payment and scheduled payment/transfer by customer.

c) implement surveillance mechanism with alert triggering and handling processes to detect potential security risks associated with mobile devices (e.g. rooted/jailbroken devices). Authorized institutions should clearly warn customers of the risks associated with using such devices before allowing customers to access mobile banking services or even consider restricting such devices from accessing mobile banking service; and

d) send an additional notification to the customers immediately via other registered communication channel that is different from the original notification channel if the original notification is generally accessible by mobile devices once the customer initiates a high-risk transaction or a small-value funds transfer to an unregistered payee.

Specific electronic banking channels

4.13 In addition to the controls generally applicable to internet banking (paragraphs 4.1 – 4.12), authorized institutions should implement additional security measures given under paragraphs 4.14 to 4.16 below to address the risks of **Social Media Platforms, Self-service Terminals,** and **Phone Banking** if relevant delivery channels are offered to customers.

4.14 When allowing the banking services to be accessed through the **Social Media Platforms**, authorized institutions will be exposed to several types of risks, including but not limited to the customer data breach arising from insecure interface or connections, the system intrusion caused by the security vulnerabilities of the platforms, reputational risk due to the service interruption and inappropriate customer dispute handling caused by the platform. Authorized institutions should implement the following measures before partnering with the social media platforms/portals:

a) assess the suitability of partnership with the platforms/portals in terms of their financial status, adequacy of risk management controls, and the record in preventing data breaches;

b) conduct legal due diligence to ensure the compliance with applicable local or overseas legal or regulatory requirements;

c) implement adequate security controls and conduct periodic assessment to minimize the risk of intrusion into the electronic banking systems and networks of authorized institutions, and the risk of customer data leakage during the data transmission process; and

d) ensure appropriate arrangements in place to properly follow-up customer complaints and apportionment of liability for possible financial losses caused by the issues involving the platforms/portals.

4.15 When allowing the banking services to be accessed through the **Self-service Terminals**, authorized institutions should conduct periodic assessment to identify and evaluate the

risks which include but not limited to card skimming attacks, unauthorized access and control to the terminals, and failure to detect and handle the counterfeit banknotes. Appropriate risk management measures should be implemented to address the associated risks. In addition, emerging cyber-attacks and vulnerabilities associated with self-service terminals should be monitored closely and proper measures should be taken to address the risks by the authorized institutions.

4.16 Adequate customer identity authentication controls should be implemented in **Phone Banking** operations to minimize the risk of customer impersonation. The common authentication methods include phone banking passwords, biometric authentication, and identity verification questions. Authorized institutions should be aware of the risks that may weaken the effectiveness of the authentication methods (e.g. the answers to identity verification questions are available from public sources) and deploy additional measures if needed. The additional measures may include asking questions with dynamic answers such as information related to recent transaction. In cases where phone banking services allow high-risk transactions, 2FA should be implemented to authenticate the identity of the customers. In addition, authorized institutions should implement proper controls (e.g. giving access to customer information on a need-to-know basis, and maintaining the access records to the identity verification questions and answers) to address the risks that staff (or service providers) who have access to the answers of the identity verification questions may use the information to impersonate the customer.

Customer Security

4.17 It is the primary responsibility of authorized institutions to ensure that the customer security through electronic banking channels is maintained at the level at which traditional banking distribution channels are used. In particular, authorized institutions shall enhance customer security with sufficient advice and awareness program, timely notification, effective precautionary measure against suspicious or fraudulent sources, appropriate information disclosure and customer data privacy protection as given under paragraphs 4.18 to 4.22 below.

4.18 Authorized institutions' security risks may be heightened if their customers do not know or understand the necessary security precautions relating to the use of electronic banking services. To complement the aforementioned security controls, authorized institutions should regularly provide easy-to-understand advice (e.g. this may cover the selection and protection of passwords, safeguards against electronic banking frauds, reminding customers not to access electronic banking through public or shared computers and unsafe network, precautions on fraudulent emails/websites/SMS/mobile application, and protection from viruses and malicious program, etc.) to their customers

on electronic banking security precautions through various channels[18] and oblige them of their responsibilities to take reasonable measures[19]. Customer education and awareness program should be tailored to minimize the risks from the misuse of specific delivery channels (e.g. mobile devices).

4.19 In the event of any high-risk transaction conducted through electronic banking system, timely notification(s) should be delivered to customers via pre-registered channels to detect unauthorized transaction(s). Each 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. Customers may choose to opt out from "trade execution" notifications. In this case, authorized institutions should provide adequate risk disclosure to the customers and obtain customers' acknowledgment of the risks involved.

4.20 Precautionary measures against fraudulent websites, e-mails, SMS, mobile applications, social media accounts or phone calls, include giving reminders to their customers that sensitive account and personal information will not be asked via online channels (e.g. emails, hyperlink, SMS, attachment) or incoming phone call; and customers should not access electronic banking accounts through hyperlinks embedded in emails, SMS or internet search engines. Authorized institutions should search for fraudulent websites or mobile applications actively and regularly and keep themselves alert of such existences. Authorized institutions should establish ongoing communication channels to notify the customers of any fraudulent or unreliable sources. In case authorized institutions find any fraudulent website or mobile application that looks similar to their own, they are expected to:

a) report the case to the Judiciary Police/the Cybersecurity Incident Alert and Response Centre (CARIC) and the AMCM;

b) take proper remediation actions such as making attempts to remove fraudulent or fake items;

c) notify customers in a timely manner via various channels of such fraudulent or fake items and clarify that they have no connection with the fraudulent website or mobile application and, in case there were emails or SMS containing hyperlink to the fraudulent website or mobile app, that they have not sent such emails or SMS; and

d) ask the customers who have conducted financial transactions through the website or mobile application to contact them[20] for remedial actions.

---

18 Channels may include face-to-face communication, social media platforms, official website, mobile applications, SMS, emails, promotional videos or leaflets, etc.

19 For example, to install anti-virus, anti-spyware and firewall software on their personal computers and mobile devices, to update the anti-virus and firewall products with security patches or newer versions on a regular basis, etc.

20 Authorized institutions shall equip their staff with the necessary information and knowledge to answer customers' enquiries effectively.

4.21 **Information disclosures.** Authorized institutions should ensure that adequate information is disclosed to avoid customer confusion and to allow potential customers to make a determination of the authorized institutions' identity and regulatory status prior to using electronic banking service. For example, the information that an authorized institution may provide to its customers/potential customers on its website or mobile application includes but not limited to:

a) the name of the authorized institution and the location of its head office (and branch offices if applicable);

b) the identity of the primary supervisory authority responsible for the supervision of the authorized institution's head office (this means the AMCM in the case of authorized institutions incorporated in Macao);

c) instructions on how customers can contact the authorized institution's customer service center regarding service problems, enquiries, complaints, suspected misuse of accounts, etc.;

d) the terms and conditions applying to electronic banking products and services, which should set out clearly the respective fees, rights, obligations and responsibilities between the authorized institution and its customers;

e) the authorized institution's customer privacy, security policy and security measures and reasonable precautions customers should take when accessing their online accounts (see also paragraph 4.22 below);

f) the jurisdictions to which the authorized institution intends to provide electronic banking services or, conversely, the jurisdictions to which it does not intend to provide its products and services; and

g) other information that may be appropriate or required by specific jurisdictions.

4.22 **Customer privacy and confidentiality.** Maintaining the privacy of a customer's information is a key responsibility for an authorized institution. Authorized institutions should ensure that their privacy policies and standards comply with applicable privacy laws and regulations. For example, reasonable endeavors should be made to ensure that:

a) the authorized institution's customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing electronic banking products and services;

b) customers are informed of the authorized institution's privacy policies and relevant privacy issues concerning the use of electronic banking products and services;

c) risks associated with sensitive information retrieved and/or processed by authorized institution (e.g. biometric data such as fingerprint/iris patterns/facial images) are prominently disclosed;

d) customers may disallow the authorized institution to share with a third party for cross-marketing purposes any information about the customer's contact details, sensitive data (such as identity card number, credit/debit card number, bank accounts information), personal needs, interests, financial position, payment or banking activity;

e) customer data are not used for purposes beyond which they are specifically allowed or for purposes beyond which customers have authorized; and

f) the authorized institution's standards for customer data usage must be met when third parties have access to customer data through outsourcing relationships.

Additional sound practices for maintaining the privacy of customers' electronic banking information can also be found from Appendix V of the Basel Committee's paper "Risk Management Principles for Electronic Banking" (http://www.bis.org/publ/bcbs98.htm).

5 FRAUD MONITORING

5.1 Due to the growing complexities of fraud techniques and sophisticated tactics, fraud monitoring is of great significance for protecting customers from the potential losses caused by fraudulent behaviours and activities. An effective fraud monitoring mechanism [21] should be established to prevent, detect and block exceptional transactions or unusual activities in a timely manner. Authorized institutions should also closely monitor the trends and developments of fraudulent techniques, and regularly enhance the fraud monitoring mechanism whenever there is a need. Any reported fraud incidents, latest threats and intelligence gathered from internal and external sources should be taken into consideration during the process.

5.2 Fraud handling process and procedure should be formally defined and documented in order to promptly verify and respond to fraud incidents. The process and procedure should include prevention and remediation measures to deal with suspected frauds, exceptional transactions or alerts generated by the fraud monitoring mechanism (e.g. suspend high-risk or suspicious transactions for screening and evaluation purposes, identify possible root causes, escalate incidents promptly to management). In addition, authorized institution should promptly contact the customers to verify the transactions or activities through a reliable channel whenever there is a need.

[21] The mechanism should include consideration of, for example, service access from suspicious sources (e.g. Internet Protocol address), abnormal customer behaviours (e.g. user access to the service via infrequently-used devices, cash withdrawals from ATM in different countries or regions within a short period of time, frequent fund transfers to the same payee(s) or cash withdrawals within a short period of time), abnormal subsequent activities (e.g. changing contact details shortly after the opening of internet banking/mobile banking account, changing customer's mobile phone number shortly followed by large value transfer to unregistered payee) and other known fraudulent scenarios.

5.3 Authorized institutions should allocate sufficient resources and designated staff with relevant expertise on fraud monitoring and response. Continuous training should be provided for such staff to keep their knowledge and skill level up-to-date with emerging threats, trends, and techniques in fraud risk management.

6 BUSINESS CONTINUITY PLANNING

6.1 **Effective capacity, business continuity and contingency planning.** Interruption in services may significantly affect electronic banking customers, who often expect 7x24 availability. Due to the potential impact (e.g. bill and other payment transactions cannot be executed on time) on customers and customer service, authorized institutions should analyze the impact of service outages and take steps to decrease the probability of outages and minimize the recovery time. For example, authorized institutions should:

- conduct regular capacity planning exercise with reference to the estimated future transaction volume or business growth over the electronic banking systems, and review the network and system architecture design to identify the corresponding dependencies in supporting the system;
- implement measures (e.g. high availability architecture, traffic controls) to ensure the availability of electronic banking systems;
- perform end-to-end performance tests[22] over critical electronic banking systems and relevant supporting network and system infrastructure by simulating various load scenarios prior to the launch of new electronic banking services and major system changes to identify potential performance bottlenecks;
- implement automated performance monitoring and alert mechanisms, which cover all critical electronic banking systems and relevant supporting network and system infrastructure, so that any potential service interruption or performance deterioration could be detected and handled in a timely manner; and
- establish appropriate business continuity and contingency plans[23] for critical electronic banking processing and delivery systems which should be regularly tested.

Other sound capacity, business continuity and contingency planning practices can be found from Appendix VI of the Basel Committee's paper "Risk Management Principles for Electronic Banking" (http://www.bis.org/publ/bcbs98.htm).

---

22 In some circumstances, the test may be performed in a "production-like" test environment if the existing services are having major enhancements or subject to 7x24 services.

23 In light of the activity volumes, number of customers affected, and the availability of alternate service channels, some institutions may not consider electronic banking services as "mission critical" warranting a high priority in its business continuity plan. Management should periodically reassess this decision to ensure that the supporting rationale continues to reflect the actual growth and strategy for growing and/or expanding its electronic banking services.

6.2 **Incident response and management.** Authorized institutions should develop appropriate incident response plans and procedures to manage, contain and minimize problems arising from unexpected events, including internal and external attacks that may hamper the provision of electronic banking systems and services. An effective incident response should include:

- plans to address recovery of electronic banking systems and services;
- mechanisms to identify an incident or crisis as soon as it occurs and to assess its materiality and impact;
- an incident response team with the authority to act in an emergency and sufficiently trained in analyzing incident detection/response systems, interpreting the significance of related output and determining the appropriate action to be taken;
- a clear chain of command, encompassing both internal as well as outsourced operations (e.g. escalation and internal communication procedures to notify senior management);
- a process for alerting the AMCM, Cybersecurity Incident Alert and Response Centre (CARIC) and other relevant authorities in the event of material security breaches or disruptive incidents;
- a communication strategy to adequately address the concerns of external parties (e.g. customers, media and business partners);
- a process for collecting and preserving forensic evidence to facilitate the subsequent reviews and prosecution of attackers; and
- regular drills of the incident response plan for electronic banking systems to ensure the effectiveness of the plan and familiarity with the handling procedures set out in the plan.

6.3 **Notification when institutions face disruption of service.** Authorized institutions should proactively notify customers who are affected or likely to be affected via effective channels after detecting incidents. When the disruption of service [24] is estimated to last for a prolonged period of time, authorized institutions should take more effective measures such as issuing a press release and provide ongoing communications to customers with incident updates (e.g. estimated impact, affected service, expected recovery time, alternative service delivery channels, etc.).

7 OUTSOURCING MANAGEMENT

[24] Authorized institutions should adopt the relevant notification controls as outlined in the AMCM's "Guideline on Business Continuity Management", where applicable.

7.1 It has become quite common for authorized institutions to outsource certain parts or all of their electronic banking operations[25], to an affiliate or third party service providers. Whatever the reasons for outsourcing, authorized institutions should note that their responsibilities and accountabilities would not be diminished or relieved by the outsourcing of their operations. Specifically, their duty to maintain secrecy under the Financial System Act, the Personal Data Protection Law and other statutory provisions will continue to apply to them after outsourcing. Authorized institutions should therefore provide effective oversight of the service providers' activities to identify and control the resulting risks and to ensure that their outsourcing arrangements are in compliance with relevant statutory requirements. Authorized institutions are expected to adopt the sound practices on outsourcing as given under paragraphs 7.2 to 7.7 below[26]. Additional sound practices for managing outsourced electronic banking systems can also be found from Appendix II of the Basel Committee's paper "Risk Management Principles for Electronic Banking" (http://www.bis.org/publ/bcbs98.htm).

7.2 Authorized institutions should understand fully the risks associated with entering into an outsourcing arrangement. Before a service provider is appointed, due diligence should be carried out to consider the service provider's financial condition, risk profile, experience, expertise, technological compatibility, and customer satisfaction.

7.3 There should be a formal contract between the authorized institution and the service provider. The terms and conditions governing the roles, relationships, obligations and responsibilities of the concerned parties should be carefully and properly defined in writing. Examples of the contract issues include:

(a) restrictions on use of non-public customer information collected or stored by the service provider;

(b) requirements for appropriate controls to protect the security of customer information held by the service provider and, ownership of the information after expiration or termination of the contract;

(c) service-level standards such as website / mobile application up-time, hyperlink performance, customer service response times, etc.;

(d) incident response plans, including notification responsibilities, to respond to website/mobile application outage, defacement, unauthorized access, or malicious code;

---

[25] The operations to be outsourced may include information system hosting (e.g. software application, websites), information systems operation and maintenance (e.g. processing and handling of system or application data; monitoring and maintenance of data centres, hardware or local area networks), middle and back-office operations (e.g. electronic fund transfer, customer service, call-centre maintenance), white-labelling arrangements, business continuity and disaster recovery functions.

[26] Authorized institutions should adopt the additional controls as outlined in the AMCM's "Guideline on Outsourcing" and relevant Industry Guidance, as necessary.

(e) business continuity plans for electronic banking services including alternate processing lines, backup servers, emergency operating procedures, etc.;

(f) provisions for the conduct of independent reviews and/or audits of security, internal controls and business continuity and contingency plans;

(g) limitations on subcontracting of services, either domestically or internationally; and

(h) choice of law and jurisdiction for dispute resolution and access to information by the authorized institution and relevant regulators.

7.4 Authorized institutions should require service providers to implement security policies, procedures and controls that are at least as stringent as the authorized institutions would expect for their own operations. They should also require service providers to develop and implement viable contingency and business continuity plans to ensure the continuity of their service and performance. Such plans should be reviewed, updated, and tested regularly by the service providers in accordance with changing technological conditions and operational requirements.

7.5 On a regular basis (depending on actual needs), authorized institutions should conduct due diligence reviews to evaluate whether service providers are capable of delivering the level of performance, able to maintain an adequate level of security, and keep abreast of the rapidly changing technology. Appropriate processes should also be established to monitor the service provider's financial condition and risk profile, and contract compliance. Authorized institutions should track the performance of the services provided and/or any security problems or the service provider's financial conditions and risk profile through online or periodic written reports from service providers. The information to be required includes, but not limited to the following:

(a) **availability of service** – e.g. statistics regarding the frequency and duration of service disruption (including the reasons for disruptions), "up time" and "down time" percentages; and volume and type of access problems reported by customers;

(b) **level and volumes of activities** – e.g. number of accounts serviced in different electronic banking channels (such as web application, mobile application, etc.), frequency of APIs requested, number and percentage of new, active or inactive accounts; and type, number and value of transactions;

(c) **efficiency of performance** – e.g. average response times by time of day, server capacity utilization, type of customer service enquiry and average time to resolution;

(d) **incidents on security** – e.g. volume of rejected log-on attempts, password resets, attempted and successful penetration attempts, number and type of trapped viruses or other malicious code, and any physical security breaches;

(e) **stability of service provider** - e.g. quarterly or annual financial reports, number of new or departing customers, changes in systems, employee turnover and changes in management positions; and

(f) **assurance on quality** - e.g. reports on performance, audit results, penetration tests, and vulnerability assessments.

7.6 Throughout the course of outsourcing, authorized institutions should have contingency plans in place to prepare for the possibility that the current service providers might not be able to continue operations or render the services required. Such plans should also cater for the need to change the service providers or the service relationship due to substandard performance of the service providers or any other problems identified in the above due diligence process.

7.7 Regular audits of the outsourced operations will help ensure that relevant controls are appropriate and functioning properly. In addition to the abovementioned oversight processes, authorized institutions should ensure that periodic independent internal and/or external audits are conducted on the outsourced operations to at least the same scope required if such operations were conducted in-house.

8 MANAGEMENT OF CROSS-BORDER ACTIVITIES

8.1 Taking advantage of the open, ubiquitous and automated nature of the Internet, many international institutions are providing electronic banking products and services to their customers in different countries/jurisdictions through the web sites / mobile applications of their branches or subsidiaries in those countries. Some other institutions have also begun to conduct electronic banking activities remotely from one jurisdiction to residents in another jurisdiction where they do not already have a licensed establishment.

8.2 The Basel Committee has defined the "provision of **transactional** online products or services by an institution in one jurisdiction to customers resident in another jurisdiction" as cross-border electronic banking. Given the developments affecting issues of legal jurisdiction and choice of laws considerations with respect to cross-border commerce, institutions that engage in cross-border electronic banking may face increased legal risk. Specifically, unless institutions conduct adequate due diligence, they run the risk of potential non-compliance with different laws and regulations, including applicable consumer protection laws, advertising and disclosure laws, record-keeping and reporting requirements, privacy rules and anti-money laundering laws in foreign jurisdictions.

8.3 Accordingly, prior to engaging in **cross-border** electronic banking activities, all authorized institutions operating in Macao should **prior consult the AMCM**, which needs to be satisfied that authorized institutions have:

(a) conducted adequate and appropriate risk assessment and due diligence to ensure that they can adequately manage the attendant risks and that they comply with the laws and regulations of the foreign jurisdictions at which the electronic banking services are directed; and

(b) established an effective and ongoing risk management program for assessing, controlling, and monitoring risks arising from cross-border electronic banking activities.

8.4 These authorized institutions are also expected to define and generally mitigate their due diligence obligations by posting on their websites / mobile applications a disclaimer that limits their on-line products and services to only the residents of specified jurisdictions[27], although the legal effect of such a disclaimer might be somewhat uncertain. In addition, they should provide sufficient disclosure on their websites / mobile applications to allow potential customers to determine their identity, place of incorporation and regulatory status (see also paragraph 4.21(a)).

9 INDEPENDENT ASSESSMENTS

9.1 Given the importance of managing the risks associated with electronic banking, authorized institutions should plan for independent assessments to be conducted on their electronic banking systems before the launch of the relevant services or major enhancements to existing services. The independent assessments should, at a minimum, cover the following areas and consider the guidance in paragraphs 3 to 8 of this Guideline:

(a) board and management oversight;

(b) security controls;

(c) fraud monitoring;

(d) business continuity planning;

(e) outsourcing management; and

(f) management of cross-border activities.

9.2 As part of the independent assessment arrangement as outlined in paragraph 9.1, technical security assessment stated in paragraph 4.4 should be conducted by qualified assessor(s) to evaluate the continued effectiveness of security controls implemented on internet banking systems before the launch of the relevant services or major enhancements to existing services.

[27] Or, conversely, authorized institutions may disclose the jurisdictions to which they do not intend to provide their products and services.

9.3 In addition, penetration testing and vulnerability scanning should be performed at least annually in accordance with the requirements set out in paragraph 4.4. The scope of the penetration assessment should at least cover authorized institutions' internet banking and any financial services delivered over the internet or wireless network. Such assessment results should be submitted to the AMCM upon request, and authorized institutions should exercise prompt and proper follow-up actions based on the assessment results whenever needed.

9.4 The person(s) (i.e. the assessor) appointed by an authorized institution to perform independent assessment and technical security assessment should have, and be able to demonstrate, the necessary expertise in the relevant fields. He/she should be independent from the parties that develop or administer the electronic banking system and should not be involved in the operations to be reviewed or in selecting or implementing the relevant control measures to be reviewed. He/she should be able to report findings freely and directly to the authorized institution's senior management. As long as the assessor meets the above criteria, he/she can be the authorized institution's internal staff (e.g. internal auditors) or external party (e.g. an external auditor or other third party services providers).

9.5 Subsequent to an initial independent assessment, an authorized institution should conduct risk assessment at least every two years or when there are substantial changes to determine if further independent assessment should be required and the frequency and scope of such independent assessment. Any substantial changes to the risk profile of the services being provided, significant modifications to the network infrastructure and applications, material system vulnerabilities or major security breaches are to be taken into consideration in the risk assessment.

9.6 Reports of independent assessments should be submitted to the AMCM, which will during on-site examinations and off-site reviews use the reports as reference. In case authorized institutions have engaged different parties to conduct separate independent assessments on different aspects of their electronic banking services, they may submit either combined reports or all relevant reports separately to the AMCM. Such independent assessment reports should cover at least the following items:

(a) time of assessment and stage of development of the relevant systems (e.g. design or testing stage) up to the assessment date and the follow-up arrangement for systems being put into operation (if any) after the assessment;

(b) the scope of assessment, including descriptions of the system components, internal network, network equipment, operation and control process that are covered;

(c) assessment approach (e.g. interview, sampling, technical testing) adopted during the assessment process;

(d) the assessors' findings for independent assessment and technical security assessment (e.g. outstanding issues and impact) and recommendations (e.g. remedial measures); and

(e) management responses, including risk control measures that have been implemented or the scheduled remediation plan to address the outstanding findings.

9.7 Before offering a new electronic banking service to customers, authorized institutions should evaluate carefully the risks associated with such service, in particular, legal and reputational risk. Authorized institutions should also perform regular assessments to ensure that their controls for managing legal and reputational risks remain proper and adequate. When it is possible and appropriate, authorized institutions may take out insurance for their electronic banking activities.

10 SUPERVISORY APPROACH

10.1 In light of the possible implications regarding operational, reputational and other relevant risks, authorized institutions should notify and discuss their plans with the AMCM prior to the launch of new electronic banking services or make significant changes to existing services. In particular, prior consultation with the AMCM should take place before an authorized institution engages in cross-border electronic banking activities (see also paragraph 8.3).

10.2 The AMCM will generally require an authorized institution to present and discuss its strategic outlook for launching electronic banking services, demonstrating compatibility with the overall strategy of the authorized institution's operations, the risk analysis for the planned project together with details of risk/reward study. The management of the authorized institution is expected to demonstrate that it has reviewed the current risk profile of its operations, considered the impact of implementing an electronic service and that the board (or head office in the case of a branch of an overseas authorized institution) has concluded that there are no undue adverse implications for the safety and soundness of the operations given its resources, risk management systems and technical expertise.

10.3 Specifically, an authorized institution should satisfy the AMCM that the following issues are properly addressed:

(a) there is proper board and/or senior management oversight;

(b) major technology-related controls relevant to electronic banking have been addressed;

(c) there are appropriate security measures in place, both physical and logical together with other requisite risk management controls;

(d) relevant issues related to activities such as outsourcing and cross-border electronic banking activities have been addressed;

(e) a cost-benefit analysis has been conducted of the provision of the new electronic banking service;

(f) an electronic banking strategy, which clearly outline the policies, practices and procedures that address and control all of the risks associated with electronic banking, has been developed and documented;

(g) the effectiveness of the implementation plan will be monitored on an ongoing basis and updated periodically to take account of changes in technology, legal developments and the business environment including external and internal threats to information security; and

(h) relevant risks are monitored on an ongoing basis.

10.4 The AMCM will, in the course of its onsite examinations and offsite reviews, determine as appropriate the adequacy of authorized institutions' risk management of electronic banking services based on the requirements set out in this Guideline. Meanwhile, authorized institutions that are already offering electronic banking services are expected to ensure that their existing systems, including the arrangement for independent assessments and technical security assessments, are in compliance with this Guideline as soon as practicable and within 12 months of the date of this Guideline.