MAS

Monetary Authority of Singapore

INTERNET BANKING AND TECHNOLOGY RISK MANAGEMENT GUIDELINES

VERSION 3.0

2 JUNE 2008

TABLE OF CONTENTS

1.0 INTRODUCTION

1.0.1 Continuing technology developments and innovations are having significant impact on the way banks interact with their customers, suppliers and counterparties, and how they undertake their operations. Banks face the challenge of adapting, innovating and responding to the opportunities posed by computer systems, telecommunications, networks and other technology-related solutions to drive their businesses in an increasingly competitive domestic and global market.

1.0.2 The internet in particular offers major opportunities for banks to reach new markets and expand the range of products and services they provide to customers. The very accessibility and dynamism of the internet brings both benefits and risks.

1.0.3 As banks rely increasingly on information technology and the internet to operate their business and interact with the markets, their awareness and recognition of the magnitude and intensification of technology risks[1] should correspondingly be more perceptive and discerning, both for individual banks and the financial industry as a whole. In this networked and market-driven environment, it is critical that banks have flexible, adaptable and responsive operating processes as well as sound and robust risk management systems.

1.0.4 The board of directors and management of a bank are responsible for managing its risks, including technology risks which are becoming more complex, dynamic and pervasive. The risk management process requires the board and management to review and appraise the cost-benefit issues on what and how much to invest in controls and security measures relating to computer systems, networks, data centres, operations and backup facilities.

[1] Technology risks relate to any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, online networks and telecommunications systems. These risks can also be associated with systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity deficiencies, network vulnerabilities, control weaknesses, security shortcomings, internal sabotage, espionage, malicious attacks, hacking incidents, fraudulent conduct and defective recovery capabilities.

1.0.5 As a general principle, a risk management framework would require the following actions to be taken:

- Identify, classify and assess risks that are relevant to the bank's operations and systems.
- Develop a documented plan containing policies, practices and procedures that address and control these risks.
- Implement and regularly test the plan.
- Monitor risks and the effectiveness of the plan on an ongoing basis.
- Update the plan periodically to take account of changes in technology, legal requirements and business environment including external and internal threats and security vulnerabilities.

1.0.6 The aim of this set of guidelines is to require banks to adopt risk management principles and security practices which will assist them in:

- Establishing a sound and robust technology risk management framework.
- Strengthening system security, reliability, availability and recoverability.
- Deploying strong cryptography and authentication mechanisms to protect customer data and transactions.

1.0.7 All banks providing internet banking[2] must erect a sound and robust risk management process that will enable them to identify, assess, measure and respond to technology risks in a proactive and effective manner.

[2] Internet banking refers to the provision of banking services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices. For the purpose of this paper, the generic reference to bank or banks includes financial institutions which provide online trading or other financial services and products on the internet and interconnected networks. Where appropriate, internet banking is to be regarded as synonymous with online financial services.

2.0 RISK MANAGEMENT FRAMEWORK

2.0.1 A sound and robust risk management framework requires the board and management to be responsible and accountable for managing and controlling technology risks. This responsibility calls for banks to perform risk analysis by identifying information systems assets, determining security threats and vulnerabilities, estimating the likelihood of exploitation or attacks, assessing potential losses associated with these risk events and taking appropriate security measures and controls for asset protection. Risk analysis is the process of examining the technology infrastructures and systems to identify possible exposures and weighing the pros and cons of different risk mitigation actions. This step requires an assessment of what damage might occur to the assets and from what sources or causes. Effective information system security controls are necessary for ensuring the confidentiality, integrity and availability of information technology resources and their associated data. These assets should be adequately protected from unauthorised access, deliberate misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure. Risks that are deemed material to the organisation should be thoroughly evaluated and prioritised to enable a strategy to be developed for addressing and mitigating these risks.

2.0.2 Due to the open and complex nature of the internet, the risks associated with using this infrastructure for electronic banking are accentuated. Banks should take this factor into account in their risk management process. A clear understanding of the interaction between the internet-based applications and the back-end support systems is required to ensure that management, operational and technical controls are effective and adequate.

2.0.3 Risk issues relating to internet banking and the launch of new products or services should be assessed and resolved during the conceptualisation and developmental stages. Risk control procedures and security measures should be put in place prior to or at the implementation phase.

2.0.4 Within the organisational structure, the board and senior management should oversee all risk management functions. On a centralised, delegated or distributed basis, this will involve relevant business, operational and support areas having technology risk management responsibilities at line or functional levels. The monitoring and reporting of risk management effectiveness and compliance should ultimately flow upwards to the chief executive officer and the board.

2.0.5 Policies, procedures and practices to define risks, stipulate responsibilities, specify security requirements, implement safeguards to protect information systems, administer internal controls and enforce compliance should be set up as essential specifications of the risk framework. Management should conduct periodic security risk assessment to identify internal and external threats that may undermine system integrity, interfere with service or result in the disruption of operations. Threat and vulnerability assessment would assist management in making decisions regarding the nature and extent of security controls required. Security awareness, training and education programmes should also be conducted internally and externally to promote and nurture a security conscious environment.

2.0.6 As part of the risk control framework, disaster recovery and business continuity planning is crucial in the development and preparation of contingency arrangements for restoring and resuming critical business operations in the aftermath of a disaster occurring at the primary computer processing site. No system is infallible or immune from mishaps. Hence, effective means to rapid recovery is critical. A bank must identify comprehensively what types of disasters are catered for in the recovery plan. Disasters can range from a total loss of service due to a natural disaster to a catastrophic system failure caused by system faults, hardware malfunction or operating errors. A substantial task in disaster recovery planning is putting together a reliable assemblage of contingency operating procedures that cover varying scenarios of operational disruption or system breakdown.

2.0.7 Periodic testing and validation of recovery requirements and readiness at the backup site should be carried out and assessed for adequacy, effectiveness and personnel ability to execute contingency procedures and restore operational capability.

2.0.8 The rapid pace of technological innovations has changed the scope, complexity and magnitude of risks that banks face in providing internet banking. Banks are required to have resilient operations and processes that enable them to manage and respond to existing risks and to adjust to new risks.

2.1 RISK MANAGEMENT PROCESS

2.1.1 The first step in any risk management process is to ascertain the value of the information system assets of the organization that should be protected. This quantitative assessment would enable the organization to rank and prioritize the information assets by value and for management to make informed business decisions on the control measures that should be implemented to protect assets. At the same time, it is essential for the organization to have a clear policy commitment to asset protection and its security goals. Different types of systems would have different values to the organization, depending on the impact to the organization if there is a loss of systems confidentiality, integrity and availability arising from attacks, vulnerability exploitation or adverse incidents.

2.1.2 A comprehensive IT security strategy is a vital component of an effective risk management process which should not be regarded as merely a technical function to be relegated to IT experts. It is an essential management function which should have the support of the top tier of management. This function involves identifying, measuring and assessing risks, as well as formulating a plan to mitigate risks down to an acceptable level.

2.2 RISK IDENTIFICATION

2.2.1 With internet banking systems, the different ways in which some of the risks arise, and their magnitude and possible consequences, take on new dimensions. Risk identification entails the determination of all kinds of threats, vulnerabilities and exposures present in the internet system configuration which is made up of components such as internal and external networks, hardware, software, applications, systems interfaces, operations and human elements.

2.2.2 During the risk identification process, consideration needs to be given to both the internet applications and their interfaces with back-end and the supporting systems. The risks and threats covering both sides together with their interdependencies should be taken into account. This aspect is important as it lays the foundation for understanding the risk and security posture of the internet applications in a more comprehensive manner.

2.2.3 Security threats such as those manifested in denial of service attacks, internal sabotage and malware infestation could cause severe disruption to the operations of a bank with consequential losses for all parties affected. Vigilant monitoring of these mutating, growing risks is a crucial step in the risk containment exercise.

2.3 RISK ASSESSMENT

2.3.1 Following the task of risk identification, the potential effect and consequences of these risks on the overall business and operations have to be analysed and quantified. In the event that certain risks are not quantifiable, management still has to define these risks and take steps to understand their potential impact and consequences should adverse incidents occur. With this information, management will then be able to prioritise the risks, perform cost-benefit analysis and make risk mitigation decisions.

2.3.2 The extent of risk impact is a function of the likelihood of various threat and vulnerability pairings or linkages capable of causing harm to the organisation should an adverse event occurs. A threat can be defined as any condition, circumstance, incident or person with the potential to cause harm by exploiting a vulnerability in a system. The source of the threat can be natural, human or environmental. Humans, with the motivation and capability for carrying out attacks, are serious sources of threats through deliberate acts or omissions which could inflict extensive harm to the organisation and its information systems. An understanding of the motivation, resources and capabilities that may be required to carry out a successful attack should be developed when sources of threats and related vulnerabilities have been identified. A particular threat does not normally pose a danger when there is no associated vulnerability to exploit in a system. This threat and vulnerability matrix may differ between organisations.

2.4 RISK TREATMENT

2.4.1 For each type of material risks identified and analysed, management should develop and implement risk mitigation and control strategies that are consistent with the value of the information asset and bank's level of risk tolerance. Risk mitigation entails a methodical approach in prioritising, evaluating and implementing appropriate risk-reduction controls and security measures which emanate from the risk assessment process. A combination of technical, procedural, operational and functional controls would usually provide a more vigorous mode of reducing security risks. As it may not be practical to address all known risks simultaneously or in the same timeframe, priority would have to be given to threat and vulnerability pairings with high risk ranking which could cause significant harm or impact. Management should also assess how much damages and losses it can withstand in the event that a given risk-related event materialises. The costs of risk controls should be balanced against the benefits to be derived.

2.4.2 It is imperative that banks are able to manage and control risks in a manner that would allow them the capacity to absorb any related losses that may eventuate without jeopardising their financial reliability and stability. When deciding on the adoption of alternative controls and security measures, management should also be conscious of their costs and effectiveness in respect of the risks being treated or mitigated. Where the threats to the safety and soundness of the system are insurmountable and the risks cannot be adequately controlled, the bank should refrain from implementing and running such a precarious system.

2.4.3 In view of the constant changes occurring in the internet environment and online delivery channels, management should institute a risk monitoring and compliance regime on an ongoing basis to ascertain the performance and effectiveness of the risk management process. When risk parameters change, the risk process needs to be updated and enhanced accordingly. Re-evaluation of past risk-control equations, renewed testing and auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken should be conducted.

2.4.4 The impact of internet banking on risk management is complex and dynamic. Management should constantly re-assess and update its risk control and mitigation approach to take into account varying circumstances and changes to its risk profile in the internet environment.

3.0 TYPES OF INTERNET FINANCIAL SERVICES

3.0.1 Due to the open and dynamic nature of the internet, the risks associated with providing online services via the internet are greater and far more extensive than closed networks and proprietary delivery channels.

3.0.2 Specific security and control measures have to be formulated to tie in with the risk management process. It is important that banks set appropriate control and security benchmarks for their internet operations.

3.0.3 The level of internet-related risk is directly linked to the type of services provided by the banks. Typically, internet financial services can be classified into information service, interactive information exchange service and transactional service.

3.1 INFORMATION SERVICE

3.1.1 This is the most basic form of online internet service. It is a one-way communication whereby information, advertisements or promotional material are provided to the customers. Many small banks choose to only provide information on the internet by setting up standalone servers or purchasing advertisement space on other websites hosted by third parties.

3.1.2 Although the risks associated with such online services are low, these websites are often the targets of hacking which vandalises and mutilates the original information being provided. A bank may suffer reputational harm resulting from its hosted website being hacked and vulgarised.

3.1.3 Where a bank purchases advertising space from a third party, regular monitoring should be made not only of the bank's advertisement, but also the associated contents of the service provider. Reputational damage may be caused by association with unsavoury advertising being hosted on the same service.

3.2 INTERACTIVE INFORMATION EXCHANGE SERVICE

3.2.1 This form of internet services offers slightly more bank-customer interactions compared with the former. Customers are able to communicate with the bank, make account enquiries and fill in application forms to take up additional services or purchase new products offered. The risks pertaining to these websites depend on whether they have any direct links to the bank's internal network. These risks range from low to moderate depending on the connectivity between the internet and the internal network and the applications that the customers could access.

3.3 TRANSACTIONAL SERVICE

3.3.1 This category of internet banking services allows customers to execute online transactions such as the transfer of funds, payment of bills and other financial transactions.

3.3.2 This is the highest risk category that requires the strongest controls since online transactions are often irrevocable once executed. The bank’s internet systems may be exposed to internal or external attacks if controls are inadequate. A heightened element of risk is that attacks against internet systems do not require physical presence at the site being attacked. At times, it is not even clear or detectable as to when and how attacks are launched from multiple locations in different countries.

4.0 SECURITY AND CONTROL OBJECTIVES

4.0.1 The internet is a global network which is intrinsically insecure. Security threats arising from denial of service attacks, spamming, spoofing, sniffing, hacking, keylogging, phishing, middleman interception, mutating virus, worms and other forms of malware pose heightened technology risk levels which banks encounter with increasing frequency and malignancy. It is imperative that banks implement strong security measures that can adequately address and control these types of risks and security threats. Banks should provide the assurance that online login access and transactions performed over the internet are adequately protected and authenticated. This would require a security strategy to be established to enable the following objectives to be met:

- Data confidentiality
- System integrity
- System availability
- Customer and transaction authenticity
- Customer protection

4.1 DATA CONFIDENTIALITY

4.1.1 Data confidentiality refers to the protection of sensitive information from prying eyes and allowing authorised access only. The bank's online systems should employ a level of encryption appropriate to the type and extent of risk present in its networks, systems and operations.

4.1.2 While a particular strength or type of encryption algorithm is not herein prescribed, it is expected that banks will properly evaluate security requirements associated with their internet systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required. In addition, banks should only select encryption algorithms which are well-established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.

4.1.3 The most important aspect of data encryption is the protection and secrecy of the cryptographic keys used, whether they are master keys, key encrypting keys or data encrypting keys. No single individual should know entirely what the keys are or have access to all the constituents making up these keys. All keys should be created, stored, distributed or changed under the most stringent conditions. The sensitivity of data and operational criticality should determine the frequency of key changes.

4.1.4 The primary application of cryptography is protecting the integrity and privacy of data for some specified time rather than ensuring their secrecy for an indefinite period. No encryption process is more secure than the host systems that run it. Hardware security modules and similar tamper-resistant devices provide the most secure way of carrying out encryption and decryption functions. Other methods may also be considered acceptable if they afford sufficient protection of encryption keys and confidential data in an end-to-end authentication operation.

4.1.5 In conformity with the general principle of data protection, the encryption security pertaining to the customer's PIN and other sensitive data should be maintained end-to-end at the application layer. This means the encryption process is kept intact from the point of data entry to the final system destination where decryption and/or authentication takes place.

4.2 SYSTEM INTEGRITY

4.2.1 System integrity refers to the accuracy, reliability and completeness of information processed, stored or transmitted between the bank and its customers. A high level of system and data integrity should be achieved consistent with the type and complexity of online services provided.

4.2.2 With internet connection to internal networks, financial systems and devices, largely determined and controlled by banks, can now be potentially accessed by anyone from anywhere at anytime. Moreover, transaction errors and operating flaws resulting from processing or transmission may remain latent and undetected for indeterminate periods as internet systems generally employ more automated processes than other less complex systems.

4.2.3 Banks should install monitoring or surveillance systems that would alert them to any erratic system activities or unusual online transactions taking place.

4.2.4 Control determinants that are pertinent to system integrity include:

- Logical access security[3]
- Physical access security[4]
- Processing and transmission controls[5]

4.3 SYSTEM AVAILABILITY

4.3.1 A high level of systems availability is required for maintaining public confidence in an online network environment. All of the previous security and control components are of little value if an online service is not available when it is needed. In broad terms, users of internet banking services expect to be able to access the online systems 24 hours every day of the year, tantamount to near zero system downtime.

4.3.2 Important factors associated with maintaining high system availability are adequate capacity, reliable performance, fast response time, scalability and swift recovery capability. Banks, their service providers and vendors who provide internet banking services need to ensure they have ample resources and capacity in terms of hardware, software and other operating capabilities to deliver consistently reliable service.

4.3.3 In the context of online banking, the interfacing support systems are just as important as the hosting system. In providing applications that are run on the internet, banks will also be using existing mainframes or backend host

[3] Logical access security is associated with how data is accessed and stored within a system or storage media. Logical access controls are preventive and detective measures that restrict a user's access to data/information to only what is permitted.

[4] Physical access security is associated with where and how systems resources, data assets and storage media are located and protected. Physical access controls include preventive measures which grant selective physical access to specific individuals.

[5] Processing and transmission controls are associated with the input, processing, communication, transmission, output, storage and retrieval of data. The controls can be preventive, detective or corrective in dealing with errors, irregularities or deviations.

systems. The same availability profile for both front-end and backend systems may be necessary to provide the level of reliability and consistency of service expected by customers.

4.3.4 Internet processing usually entails a number of complex interdependent system and network components. An entire system can become inoperable when a single critical hardware component or software module malfunctions or is damaged. Therefore, banks should maintain standby hardware, software and network components that are necessary for fast recovery.

4.3.5 Management is expected to have in place procedures and monitoring tools to track system performance, server processes, traffic volumes, transaction duration and capacity utilisation on a continual basis to ensure a high level of availability of their internet banking services.

4.4 CUSTOMER AND TRANSACTION AUTHENTICITY

4.4.1 In internet banking, cryptographic technologies play an important role in ensuring confidentiality, authenticity and integrity. Customers are required to provide their User ID and PIN combination and a one-time password (OTP), dynamic access code or digital signature so that their identity and authenticity could be verified before access to their accounts is permitted. In basic terms, this process of authentication is to validate the claimed identity of the customer by verifying "what the customer knows" (usually a password or personal identification number) and "what the customer has" (such as a hardware device which generates one-time-passwords at pre-determined time intervals or a USB token which contains a digital certificate and its associated private key).

Two factor authentication for system login and transaction authorisation can be based on any two of the following factors :

- What you know (eg. PIN)
- What you have (eg. OTP token)
- Who you are (eg. Biometrics)

4.4.2 In view of the proliferation and diversity of cyber attacks, banks should implement two-factor authentication at login for all types of internet banking systems and for authorising transactions. The principal objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating phishing, keylogging, spyware, malware, middleman attacks and other internet-based scams and malevolent exploits targeted at banks and their customers.

4.4.3 Banks should also require the repeated use of the second authentication factor (eg one-time-passwords) by the customer for high value transactions or for changes to sensitive customer data (eg customer office and home address, email and telephone contact details) during a login session. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. In the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.

4.4.4 Authentication requirements are usually achieved through the use of strong cryptography or related protocols and functions such as TripleDES, AES, RC4, IDEA, RSA, ECC, OATH and RFC 2104 HMAC. Cryptographic functions, algorithms and protocols should be used to authenticate logins and protect communication sessions between the customer and the bank. The strength of ciphers depends largely on their design, construction and the size of their keys. Constant advances in computer hardware, computational number theory, cryptanalysis and distributed brute force techniques may induce larger key lengths to be used in future. Some contemporary cipher algorithms may also have to be enhanced or replaced when they lose their potency in the face of ever increasing computer speed and power.

4.4.5 Beyond the obvious application of encryption to provide authentication and privacy of online transactions, strong cryptography provides the basis for achieving access control, transaction authorisation, data integrity and accountability. To enhance online processing security, confirmatory second channel[6] procedures should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.

4.4.6 Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes or the secure sockets layer (SSL) server certificate verification. It should be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.

4.5 CUSTOMER PROTECTION

4.5.1 Internet banking has become a mainstream and even a primary electronic delivery channel for a large number of banks. Their customers regularly log into the banks' websites to access their accounts to conduct a wide range of banking transactions for personal and business purposes. However, the popularity and world-wide accessibility of internet banking have attracted a growing list of internet hacking threats and exploits.

4.5.2 Customer protection is of paramount importance in internet banking. The bank must ensure that a customer is properly identified and authenticated before access to sensitive customer information or online banking functions is permitted. Sensitive customer information includes customer personal particulars or account details that could be used to identify a customer.

4.5.3 In past years, internet security threats were usually of a passive nature involving mainly eavesdropping and password guessing. In recent years, direct attacks on banking systems and customer PINs have become increasingly widespread. Through targeted attacks such as phishing, fake websites, spamming, viruses, worms, trojan horses, trapdoors, keylogging, spyware and

[6] The second channel is any communication mechanism which is separate from the internet banking system and its delivery channel. It can be telephony, SMS, email or a manual process involving paper forms and handwritten signatures.

middleman infiltration, customer PINs are under constant threats from various types of systems vulnerabilities, security flaws, exploits and scams.

4.5.4 The essence of two-factor authentication technology is the availability of a wide range of security tools, devices, techniques and procedures to counter the cyber threats and attacks described above. As an integral part of the two-factor authentication architecture, banks should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITMA)[7], man-in-the browser attack or man-in-the application attack (refer to appendix A for details).

4.5.5 Distributing software via the internet is becoming increasingly popular. However, in the context of internet banking, downloading and running software codes, plug-ins, applets, ActiveX programs and other executable files from anonymous or unverifiable sources is possibly one of the riskiest actions a customer could do on his personal computer. The threats and risks associated with downloading are significant if the customer could not be reasonably sure that the software is genuine and that it has not been tampered with even if it were from a legitimate source in the first instance. Many incidents have occurred where internet users have been deceived by hackers into downloading trojans, backdoors, viruses and other errant software which cause malicious damage and harmful consequences.

4.5.6 Banks should not distribute software to their customers via the internet or through a web-based system unless they can provide adequate security and safeguards for the customers. This would imply that customers can verify the provenance and integrity of the downloaded software and authenticate the bank's digital signature incorporated in the software using a digital certificate provided by the bank. In return, the bank is also able to check the authenticity and integrity of the software being used by the customers.

[7] In a man-in-the-middle attack, an interloper is able to read, insert and modify at will, messages between two communicating parties without either one knowing that the link between them has been compromised. Possible attack points for MITMA could be customer computers, internal networks, information service providers, web servers or anywhere in the internet along the path between the user and the bank’s server.

5.0 SECURITY PRINCIPLES AND PRACTICES

5.0.1 Security principles and practices can limit the risk of external and internal threats against the security and integrity of internet based systems. When properly implemented and adhered to, they also safeguard the authenticity and confidentiality of data and operating processes.

5.0.2 Security practices usually involve combinations of hardware and software tools, administrative procedures and personnel management functions that contribute to building secure systems and operations. These security principles, practices and procedures are collectively known as the security policy functions and processes of an organisation.

5.1 HUMAN RESOURCE MANAGEMENT

5.1.1 Internet security ultimately relies on trusting a small group of skilled personnel, who must be subject to proper checks and balances. Their duties and access to systems resources for the more reason must be placed under close scrutiny. It is important that stringent selection criteria and thorough screening is applied in appointing personnel to internet operations and security functions. Personnel involved in developing, maintaining and operating websites and systems should be adequately trained in security principles and practices.

5.1.2 Three of the most basic internal security principles[8] for protecting systems are:

a) Never alone principle

Certain systems functions and procedures are of such sensitive and critical nature that they should be jointly carried out by more than one person or performed by one person and immediately checked by another. These functions include systems initialisation, network security configuration, access control system installation, changing operating system parameters, implementing

[8] These internal control principles can be adapted depending on separation of responsibilities, division of duties, environmental variables, systems configurations and compensating controls. Where relevant, physical security is imputed in applicable control principles and practices.

firewalls and intrusion prevention systems, modifying contingency plans, invoking emergency procedures, obtaining access to backup recovery resources as well as creating master passwords and cryptographic keys.

b) Segregation of duties principle

Segregation of duties is an essential element of internal controls. Responsibilities and duties that should be separated and performed by different groups of personnel are operating systems function, systems design and development, application maintenance programming, computer operations, database administration, access control administration, data security, librarian and backup data file custody. It is also desirable that job rotation and cross training for security administration functions 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 processing details to be concealed.

c) Access control principle

Access rights and system privileges must be based on job responsibility and the necessity to have them to fulfil one's duties. 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 authorisation should be allowed to access confidential information and use system resources solely for legitimate purposes.

5.1.3 Internal sabotage, clandestine espionage or furtive attacks by trusted employees, contractors and vendors are potentially among the most serious risks that a bank faces. Current and past employees, contractors, vendors and those who have an intimate knowledge of the inner workings of the bank's systems, operations and internal controls have a significant advantage over external attackers. A successful attack could potentially jeopardise customer confidence in a bank's internal control systems and processes.

5.1.4 No one should have concurrent access to both production systems and backup systems, particularly data files and computer facilities. Any person who needs to access backup files or system recovery resources should be duly authorised for a specific reason and a specified time only. Access which is not for a specific purpose and for a defined period should not be granted.

5.1.5 Personnel from vendors and service providers, including consultants, who have been given authorised access to the organisation's critical network and computer resources pose similar risks. These external personnel should also be subject to close supervision, monitoring and access restrictions similar to those applying to internal personnel.

5.1.6 Some of the common tactics used by insiders include planting logic bombs; installing stealth scripts; creating system backdoors to gain unauthorised access; as well as sniffing and cracking passwords. System administrators[9], IT security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the internet banking systems they maintain or operate by virtue of their job functions and privileged access.

5.1.7 Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged as they have the inside knowledge and the resources to circumvent systems controls and security procedures. Adoption of the control and security practices enumerated below is recommended:

- implement two-factor authentication for privileged users;
- institute strong controls over remote access by privileged users;
- restrict the number of privileged users;
- grant privileged access on a “need-to-have” basis;
- maintain audit logging of system activities performed by privileged users;
- ensure that privileged users do not have access to systems logs in which their activities are being captured;
- conduct regular audit or management review of the logs;
- prohibit sharing of privileged IDs and their access codes;
- disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and
- protect backup data from unauthorised access.

[9] For the purpose of this document, system administrators refer to personnel who are granted privileged access to maintain or operate systems, computer equipment, network devices, security tools, databases and applications.

5.2 SECURITY PRACTICES

5.2.1 Banks should conform to the following security practices:

a) Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.

b) Install firewalls between internal and external networks as well as between geographically separate sites.

c) Install intrusion detection-prevention devices (including denial-of-service security appliances where appropriate).

d) Develop built-in redundancies for single points of failure which can bring down the entire network.

e) Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.

f) Engage independent security specialists[10] to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff who are operationally or functionally responsible for the system or activity.

g) Conduct penetration testing at least annually.

h) Establish network surveillance and security monitoring procedures with the use of network scanners, intrusion detectors and security alerts.

[10] Throughout this document, independence has a functional meaning in that a review or assessment can be carried out by proficient and competent specialists or auditors who are not operationally responsible for the function, work or task being reviewed, audited or assessed.

i) Implement anti-virus software.

j) Conduct regular system and network configurations review and data integrity checks.

k) Maintain access security logs and audit trails.

l) Analyse security logs for suspicious traffic and intrusion attempts.

m) Establish an incident management and response plan.

n) Test the predetermined response plan relating to security incidents.

o) Install network analysers which can assist in determining the nature of an attack and help in containing such an attack.

p) Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.

q) Maintain a rapid recovery capability.

r) Conduct security awareness education and programs.

s) Require frequent ICT audits to be conducted by security professionals or internal auditors who have the requisite skills.

t) Consider taking insurance cover for various insurable risks, including recovery and restitution costs.

u) Provide separate physical/logical environments for systems development, testing, staging and production; connect only the production environment to the internet.

v) Implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.

w) Implement two-factor authentication at login for all types of internet banking systems and a specific OTP or digital signature for each value transaction above a specified amount selectable by the customer or pre-determined by the bank.

x) Deploy strong cryptography and end-to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.

y) Encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

z) Deploy strong user authentication in wireless local area networks and protect sensitive data with strong encryption and integrity controls.

6.0 SYSTEM DEVELOPMENT AND TESTING

6.0.1 Many systems fail because of bad system design and inadequate testing. System defects and deficiencies should be caught early at the system design stage or during testing. For major projects, a steering committee, consisting of various management, development and user stakeholders should be established to provide oversight and to monitor the progress of the project, including the deliverables to be realised at each phase of the project and the milestones to be reached according to the project timetable.

6.1 SYSTEM DEVELOPMENT LIFE CYCLE

6.1.1 In the system development life cycle framework, the tasks and processes for developing or acquiring new systems should include the assignment and delineation of responsibilities and accountabilities for system deliverables and project milestones. User functional requirements, systems design and technical specifications and service performance expectation should be adequately documented and approved at appropriate management levels.

6.1.2 Besides business functionalities, security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, security event tracking and exception handling are required to be clearly specified. A compliance check against the bank's security standards and regulatory requirements would be expected.

6.1.3 A methodology approved by management should set out how and what system testing[11] should be conducted. The scope of the tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions. Full regression testing is required to be performed before major system rectification or enhancement is implemented. The outcome of the tests should be reviewed and signed off by the users whose systems and operations are affected by the new changes (refer to appendix B for details on system security testing).

[11] System testing is broadly defined to include unit, modular, integration, system and user acceptance testing (UAT).

6.1.4 Penetration testing should be conducted prior to the commissioning of a new system which offers internet accessibility and open network interfaces. Its complementarity with vulnerability scanning of the external and internal network components that support the new system would be a logical outcome to expect. Vulnerability scanning should be conducted at least quarterly with penetration testing at least yearly.

6.1.5 To control the migration of new systems or changes to the production environment, it is important that separate physical or logical environments be maintained for unit, integration, system and user acceptance testing. Vendor and developer access to the UAT environment should be strictly monitored.

6.2 SOURCE CODE REVIEW

6.2.1 There are different ways of coding programs which might conceal security threats and loopholes, deliberate or unintentional. System and user acceptance testing are ineffective in detecting malicious codes, trojans, backdoors, logic bombs and other malware. No amount of black-box testing is able to identify or detect these security threats and weaknesses.

6.2.2 Source code review is a methodical examination of the source code of an application with the objective of finding security defects that are due to coding errors, insecure coding practices or malicious attempts. It is designed to detect security vulnerabilities, deficiencies, gaps and mistakes (relating to control structure, security, input validation, error handling, file update, function parameter verification, reliability, integrity, resiliency and execution etc) at the development stage and have them fixed before the system is implemented. Concurrently, code quality and programming practices can also be improved. The convenience of straight-through processing from highly integrated systems with internet front-end coupled seamlessly with back-end hosts may spawn opportunities for corrupted data or malicious codes to propagate between contiguous systems passing through one network segment to another. These types of infection, contagion and contamination may have systemic repercussions.

6.2.3 A high degree of system and data integrity is required for all internet facing applications. Banks should exercise due diligence in ensuring these applications have appropriate security controls, taking into consideration the type and complexity of online services provided.

6.2.4 Based on the bank's risk analysis, specific application modules and their security safeguards should be rigorously tested with a combination of source code review, exception testing and compliance review to identify errant coding practices and systems vulnerabilities that could lead to security problems, violations and incidents. While testing methodologies may differ for various applications, a proficient security test methodology should cover the following:

(a) Identify information leakages
Sensitive information such as cryptographic keys, account and password details, system configurations and database connection strings should not be disclosed. Potential sources of information leakages like verbose error messages and banners, hard-coded data, files and directories operations should be scrutinised for inappropriate information disclosure.

(b) Assess resiliency against input manipulation
The test should review all input validation routines and assess their effectiveness against known vulnerabilities.

(c) Identify insecure programming practices
The test should identify insecure programming practices such as use of vulnerable function calls, inadequate memory management, unchecked argument passing, inadequate logging and comments, use of relative paths, logging of passwords and authentication credentials, and inappropriate access privilege assignment.

(d) Detect deviations from design specifications
Implementation oversight is one of the common sources of vulnerabilities to an otherwise well designed application. Critical modules containing authentication and session management functions should be vetted for discrepancies between the code design and its implementation.

(e) Evaluate exception handling
When exception or abnormal conditions occur, adequate controls should be in place to ensure resulting errors do not allow users to bypass security checks or obtain core dumps. Sufficient processing details should be logged at the source of the exception to assist problem diagnosis. However, system or application details such as stack pointers should not be revealed.

(f) Evaluate cryptographic implementation

Only cryptographic modules based on authoritative standards and reputable protocols should be installed. Functions involving cryptographic algorithms and crypto-key configurations must be vetted for deficiencies and loopholes. This review should also evaluate the choice of ciphers, key sizes, key exchange control protocols, hashing functions and random number generators.

7.0 RECOVERY AND BUSINESS CONTINUITY

7.0.1 As no computer system is indestructible and its security impregnable, the need for contingency preparations and recovery capability is critical. Recovery and business resumption priorities must be defined and contingency procedures tested and practised so that business and operating disruption arising from a serious incident could be minimised. The recovery plan and incident response procedures should be evaluated periodically and updated as and when changes to business operations, systems and networks occur.

7.0.2 During a system outage, banks should refrain from adopting impromptu and untested recovery measures over pre-determined recovery actions that have been rehearsed and endorsed by management. Ad hoc recovery measures carry high operational risks as their effectiveness has not been verified through rigorous testing and validation.

7.0.3 A recovery site geographically separate from the primary site must be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site. A hotsite[12] rapid recovery capability should be created and maintained. The required speed of recovery will depend on the criticality of resuming business operations, the type of online services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers.

7.0.4 It is vital that banks include in their incident response procedures a predetermined action plan to address public relations issues. Being able to maintain customer confidence throughout a crisis period or an emergency situation is of great importance to the reputation and soundness of the bank.

7.0.5 Incident response, disaster recovery and business continuity preparations need to be regularly reviewed, updated and tested to ensure their effectiveness and that responsible staff are capable of undertaking emergency and recovery procedures when required. Recovery preparedness should fully anticipate a total shutdown or incapacitation of the primary computer site.

[12] Hotsite facility should have the operational capability and resources for achieving a recovery time objective of 4 hours or less.

7.0.6 Banks which have network and systems linked to specific service providers and vendors should conduct bilateral or multilateral recovery testing and ensure inter-dependencies are also fully catered for.

7.0.7 Having a predetermined action plan for countering and containing denial of service attacks is of paramount importance. The ability to restore normal operations swiftly and effectively following such an attack should be an integral part of the business resumption and system recovery process.

8.0 OUTSOURCING MANAGEMENT

8.0.1 In internet banking, it has become quite common for banks to outsource some or all of their computer processing, systems and administrative operations to third party service providers, hardware and software vendors, telecommunications companies, specialist firms and other support operators (generically and collectively regarded as service providers).

8.0.2 Whatever the reasons for outsourcing, which may include rapid technology deployment and accessing competencies not available internally, it is incumbent upon the banks to ensure that their service providers are capable of delivering the level of performance and service reliability, capability and security needed in their internet banking business. A bank's responsibilities and accountabilities are not diminished or relieved by outsourcing its operations to third parties or joint venture partners.

8.1 MANAGING OUTSOURCING RISKS

8.1.1 The board and senior management must fully understand the risks associated with outsourcing its internet banking operations. Before a service provider is appointed, due diligence should be carried out to determine its viability, capability, reliability, track record and financial position. The contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all the contracting parties should be carefully and properly defined in written agreements. The substance covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

8.1.2 Unless acceptable arrangements have been made and mutually agreed, the service provider should be required to provide access to all parties nominated by the bank to its systems, operations, documentation and facilities to carry out any review or assessment for regulatory, audit or compliance purpose. Notwithstanding the foregoing, the power of regulatory authorities under the Banking Act to carry out any inspection, supervision or examination of the service provider's role, responsibilities, obligations, functions, systems and facilities must be recognised in the agreements.

8.1.3 Banks and service providers must observe the requirements of banking secrecy under the Banking Act. The contracts and arrangements with service providers should take into account the need to protect the confidentiality of customer information as well as the necessity to comply with all applicable laws and regulations.

8.2 MONITORING OUTSOURCING ARRANGEMENTS

8.2.1 The bank should require the service provider to implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations. It should review and monitor the security practices and processes of the service provider on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations of the service provider. A process of monitoring service delivery, performance reliability and processing capacity of the service provider should also be established for the purpose of gauging ongoing compliance with agreed service levels and the viability of its operations.

8.2.2 As the bank's outsourcing relationships and dependencies increase in complexity and importance, a rigorous risk management approach should be adopted to ensure management's responsibilities for protecting the bank's core operations and services are not dissipated.

8.3 CONTINGENCY AND BUSINESS CONTINUITY PLANNING

8.3.1 Management should require the service provider to develop and establish a disaster recovery contingency framework which defines its role and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures. As human error still accounts for the bulk of systems downtime and failures, all parties and personnel concerned should receive regular training in activating the contingency plan and executing the recovery procedures. This plan should be reviewed, updated and tested regularly in accordance with changing technology conditions and operational requirements.

8.3.2 The bank should also put in place a contingency plan based on credible worst-case scenarios for service interruptions to prepare for the possibility that its current service provider might not be able to continue operations or render the services required. It should incorporate identification of viable alternatives for resuming its internet banking operations elsewhere.

9.0 DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)

9.0.1 Although Distributed Denial of Service (DDoS) attacks have always posed a formidable threat to internet banking systems, the proliferation of botnets[13] and the advent of new attack vectors together with the rapid adoption of broadband globally in recent years have fuelled the potency of such attacks.

9.0.2 The normal amount of network bandwidth and system capacity sizing of even a large commercial organisation is unlikely to withstand a sustained DDoS offensive by a sizeable botnet or a group of botnets. The immense quantity of computing resources amassed by botnets to unleash an attack would rapidly deplete the network bandwidth and processing resources of a targeted system, inevitably inflicting massive service disruption or cessation.

9.0.3 Notwithstanding that most banks have instituted effective safeguards to protect their systems from trojan and worm infections, which may cause them to become unwitting members of botnets, more should be done to bolster system robustness against DDoS attacks. In this regard, banks are expected to have in place a strategy to address the botnet threats.

9.1 DETECTING AND RESPONDING TO ATTACKS

9.1.1 Banks providing internet banking should be responsive to unusual[14] network traffic conditions, volatile system performance or a sudden surge in system resource utilisation as these may be symptomatic of a DDoS onslaught. Consequently, the success of any pre-emptive and reactive actions hinges on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.

[13] Botnets are swarms or hordes of computers which have been infected with malicious software, operating under a common command and control infrastructure. A botnet master is able to enlist the compromised machines to launch a DDOS attack.

[14] A baseline for normal system processes, indicators and traffic patterns should be used as a guide for identifying unusual system behaviour.

9.1.2 As part of the defence strategy, banks should install and configure firewalls, intrusion detection/preventions systems, routers and other specialised network equipment to alert security personnel and divert and/or filter network traffic in real-time once an attack is suspected or confirmed. Due to the significant volume of traffic that needs to be processed, the use of purpose-built appliances designed for high-speed performance should be considered. The objective here is to remove malicious packets so that legitimate traffic en route to the internet banking systems could flow through.

9.1.3 Potential bottlenecks and single points of failure vulnerable to DDoS attacks could be identified through source code review, network design analysis and configuration testing. The elimination of these weaknesses would improve system resilience.

9.2 SELECTION OF INTERNET SERVICE PROVIDERS

9.2.1 Without the co-operation of internet service providers (ISPs), many organisations find the task of foiling DDoS attacks daunting. An effective countermeasure would often rely on the ISPs to dampen an attack in upstream networks.

9.2.2 Given that a collaborative approach should be adopted by banks and their ISPs, it is important that banks incorporate DDoS attack considerations in their ISP selection process which should include determining:

- whether an ISP offers DDoS protection or clean pipe services to assist in detecting and deflecting malicious traffic;
- the ability of the ISP to scale up network bandwidth on demand;
- the adequacy of an ISP’s incident response plan; and
- the ISP’s capability and readiness in responding quickly to an attack.

9.3 INCIDENT RESPONSE PLANNING

9.3.1 An incident response framework should be devised and routinely validated to facilitate fast response to a DDoS onslaught or an imminent attack. This framework should include a plan detailing the immediate steps to be taken to counter an attack, invoke escalation procedures, activate service continuity arrangements, trigger customer alerts, as well as report to MAS and other authorities.

9.3.2 Banks should be familiar with the ISPs' incident response plans and assimilate them into their incident response framework. To foster better co-ordination, banks should establish a communication protocol with their ISPs and conduct periodic joint incident response exercises.

10.0 BANK DISCLOSURE

10.0.1 Banks should provide clear information to their customers about the risks and benefits of using internet banking before they subscribe to internet banking services. Customers should be informed clearly and precisely on the respective rights, obligations and responsibilities of the customers and the bank on all matters relating to online transactions, and in particular, any problems that may arise from processing errors and security breaches. Information written in prolix legalese and technical terminology would cause legibility and comprehension difficulties for customers.

10.0.2 The terms and conditions applying to online banking products and services should be readily available to customers within the internet banking application. On initial logon or subscription to a particular service or product, this would require a positive acknowledgement of the terms and conditions from the customer.

10.0.3 Banks should publish their customer privacy and security policy. Customer dispute handling, reporting and resolution procedures, including the expected timing for the banks' response, should also be clearly defined. All this information should be posted on the banks' websites. Disclosure of information should be useful and relevant for the customers in making informed decisions.

10.0.4 On their websites, banks should advise and explain to their customers the security measures and reasonable precautions customers should take when accessing their online accounts. The precautionary procedures would include taking adequate steps to prevent unauthorised transactions and fraudulent use of their accounts, as well as making sure that no one else would be able to observe or steal their access credentials or other security information to impersonate them or obtain unauthorised access to their online accounts.

10.0.5 On the contingency that security breaches may occur and customer online accounts might have been fraudulently accessed and unauthorised transactions made, banks should explain on their websites what process will be invoked to resolve the problem or dispute, as well as the conditions and circumstances in which the resultant losses or damages would be attributable to the banks or their customers.

11.0 CUSTOMER EDUCATION

11.0.1 The importance of educating customers on the security and reliability of their interaction with the bank should not be underestimated. Customer's confidence in the safety and soundness of the bank's online products and services depends to a large extent on their understanding of and compliance with the security requirements connected with the operation of their banking accounts and transaction services.

11.0.2 Customer education may include web-based online education or other media whereby a guided learning experience may be defined. When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank should ensure that customers have sufficient instruction and information to be able to properly utilise them. Continual education and timely information provided to customers will help them to understand security requirements and take appropriate steps in reporting security problems.

11.0.3 To raise security awareness, banks should exhort customers on the need to protect their PINs, security tokens, personal details and other confidential data. PIN and OTP security instructions should be displayed prominently in the user login page or the USER ID, PIN and OTP entry page. The following advice would be instructive in helping customers to construct robust PINs and adopt better security procedures:

- PIN should be at least 6 digits or 6 alphanumeric characters, without repeating any digit or character more than once.

- PIN should not be based on user-id, personal telephone number, birthday or other personal information.

- PIN must be kept confidential and not be divulged to anyone.

- PIN must be memorised and not be recorded anywhere.

- PIN should be changed regularly.

- The same PIN should not be used for different websites, applications or services, particularly when they relate to different entities.

- Customer should not select the browser option for storing or retaining user name and password.

- Customer should check the authenticity of the bank's website by comparing the URL and the bank's name in its digital certificate or by observing the indicators provided by an extended validation certificate.

- Customer should check that the bank's website address changes from http:// to https:// and a security icon that looks like a lock or key appear when authentication and encryption is expected.

- Customer should not allow anyone to keep, use or tamper with his OTP security token.

- Customer should not reveal the OTP generated by his security token to anyone.

- Customer should not divulge the serial number of his security token to anyone.

- Customer should check his bank account balance and transactions frequently and report any discrepancy.

11.0.4 Customers should be advised to adopt the following security precautions and practices:

- Install anti-virus, anti-spyware and firewall software in their personal computers, particularly when they are linked via broadband connections, digital subscriber lines or cable modems.

- Update the anti-virus and firewall products with security patches or newer versions on a regular basis.

- Remove file and printer sharing in their computers, especially when they have internet access via cable modems, broadband connections or similar set-ups.

- Make regular backup of critical data.
- Consider the use of encryption technology to protect highly sensitive data.
- Log off the online session and turn off the computer when not in use.
- Do not install software or run programs of unknown origin.
- Delete junk or chain emails.
- Do not open email attachments from strangers.
- Do not disclose personal, financial or credit card information to little-known or suspect websites.
- Do not use a computer or a device which cannot be trusted.
- Do not use public or internet café computers to access online banking or perform financial transactions.

11.0.5 The above information on security precautions and good practices is not intended to be exhaustive nor static. It should be provided to customers in a user-friendly manner and updated from time to time.

11.0.6 Banks are directly responsible for the safety and soundness of the services and systems they provide to their customers. In this respect, they are required to operate and maintain adequate and effective authentication and related security systems to protect and verify their customers before access to customer bank accounts are allowed and transactions can be executed, in accordance with appropriate authorisation and validation procedures. Reciprocally, it is also important that customers take appropriate security measures to protect their devices and computer systems and ensure that their hardware or system integrity is not compromised when engaging in online banking. Customers should heed the advice of their banks in how to protect their devices or computers which they use for accessing banking services.

APPENDIX A: COUNTERING MAN-IN-THE-MIDDLE ATTACKS

A.1 As part of the two-factor authentication infrastructure, banks should also consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in-the middle attacks:

- Specific OTPs for adding new payees
  Each new payee should be authorised by the customer based on an OTP from a second channel which also shows payee details or the customer's handwritten signature from a manual procedure which is verified by the bank.

- Individual OTPs for value transactions (payments and fund transfers)
  Each value transaction or an approved list of value transactions above a certain dollar threshold determined by the customer should require a new OTP. All payment and fund transfer transactions should be encrypted at the application layer.

- OTP time window
  Challenge-based and time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend on the behaviour of the user. Due to time synchronisation problems, the use of time-based OTPs requires a time window at the server-side. Banks should not allow the OTP time window to exceed 100 seconds on either side of the server time. The smaller the time window, the lower the risk of OTP misuse.

- Payment and fund transfer security
  Digital signatures and key-based message authentication codes (KMAC) for payment or fund transfer transactions could be used for the detection of unauthorised modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him. This means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

- Second channel notification / confirmation
  The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

- Session time-out
  An online session would be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

- SSL server certificate warning
  Internet banking customers should be made aware of and shown how to react to SSL server certificate warning. They should terminate a login session if a SSL certificate does not belong to the bank and a warning is given to this effect. Customers should inform the bank immediately after logging off.

APPENDIX B: SYSTEM SECURITY TESTING

B.1 System security testing should include the following specifications:

- Information Leakage
  System information gathering is usually the first step a hacker would take by scanning and probing the perimeter of a network and the boundary of a system. At his disposal are public search engines, network scanners and specially crafted messages which could be used to find security loopholes or vulnerabilities which can be exploited to gain system entry. Tests should be carried out to detect network system verbosity and promiscuity.

- Business Logic
  Mistakes made in implementing business logic can lead to security holes whereby a user may perform an unauthorised function. For instance, a transaction operation should be performed in a certain sequence but a user can bypass controls by shuffling the sequence of input steps.

- Authentication
  The most common example of an authentication scheme is the logon process using static or dynamic passwords. Authentication testing should ensure that security requirements (credential expiry, revocation, reuse etc) are implemented correctly and the protection of security functions and cryptographic keys is robust.

- Authorisation
  After a user has been authenticated and gained access into the systems, authorisation helps to ensure that a given user is only allowed to view, write, execute, modify, create and/or delete data and invoke the functions that he is permitted to do so. Tests should be conducted to verify that the security access matrix works correctly in various permutations.

- Input Data Validation
  The most common security weakness in applications is the failure to properly validate input from the users. This weakness could spawn major vulnerabilities such as script injection and buffer overflows. Proper data validation should include the following:

i. Every input to the applications should be validated.
ii. All forms of data (such as text boxes, select boxes and hidden fields) should be checked.
iii. The handling of null and incorrect data input should be verified.
iv. Content formatting should be checked.
v. Maximum length for each input field should be validated.

- Exception/Error Handling
  Stringent exception/error handling would facilitate fail-safe processing under various error and exception conditions. Leakage of sensitive information should not be an outcome of a system failure.

- Session Management
  Manipulation of session management of applications can lead to security issues. To ensure secure session management, the following conditions should be specified:
  i. Sensitive information that is passed in the cookies is encrypted.
  ii. Session identifier should be random and unique.
  iii. Session should expire after a pre-defined length of time.

- Cryptography
  Cryptography should be employed to protect sensitive data. The strength of cryptography depends not only on the algorithm and key size, but also on its implementation. As such, the implementation must be rigorously tested covering all cryptographic functions (encryption, decryption, hashing, signing) and key management procedures (generation, distribution, installation, renewal, revocation and expiry).

- Logging
  Logging has to be implemented correctly to avoid security defects as well as facilitate follow-up investigation and troubleshooting when a system incident occurs. The requirements and specifications below would apply:
  i. Sensitive data such as passwords and authentication credentials should not be logged in transaction or system activity files.
  ii. The maximum data length for logging is pre-determined.
  iii. Successful and unsuccessful authentication attempts are logged.
  iv. Successful and unsuccessful authorisation events are logged.

- Performance and Stability
  The performance and the stability of a system under erratic conditions, such as abnormal traffic rates or frequent reboots, should be verified. Stress testing outside the stated limits of the systems should be conducted to ensure that the application still works correctly albeit with degraded service levels.

APPLICABILITY OF THESE GUIDELINES [15]

The guidelines are statements of industry best practices that institutions are encouraged to adopt. The guidelines do not affect, and should not be regarded as a statement of, the standard of care owed by institutions to their customers. Where appropriate, institutions may adapt the guidelines, taking into account the diverse activities they engage in and the different markets in which they conduct transactions. Institutions should read the guidelines in conjunction with relevant regulatory requirements and industry standards.

The objective of these guidelines is to promote the adoption of sound processes in managing technology risks and the implementation of security practices. MAS will continue to incorporate these guidelines into supervisory expectations for the purpose of assessing the adequacy of technology risk controls and security measures adopted by financial institutions. Each institution can expect that MAS will take a keen interest as to how and what extent it has achieved compliance with these guidelines.

[15] Version chronology:

Mar	2001	Version 1.0
Jul	2001	Version 1.1
Sep	2002	Version 1.2
Jun	2003	Version 2.0
Jun	2008	Version 3.0