



The Monetary Authority of Singapore

INTERNET BANKING
TECHNOLOGY RISK MANAGEMENT GUIDELINES

FEBRUARY 2001

Please forward your comments to Mr Tony Chew, Director, Technology Risk Supervision
Monetary Authority of Singapore, 10 Shenton Way MAS Building, Singapore 079117
Telephone: 2299109 Fax: 2299659 Email: tonychew@mas.gov.sg

Table of Contents

1.0 INTRODUCTION.....	1
2.0 RISK MANAGEMENT FRAMEWORK.....	2
2.1 RISK IDENTIFICATION.....	4
2.2 RISK ANALYSIS AND QUANTIFICATION	5
2.3 RISK TREATMENT	5
2.4 RISK MONITORING AND REVIEW	5
3.0 TYPES OF INTERNET FINANCIAL SERVICES.....	6
3.1 INFORMATION SERVICE.....	6
3.2 INTERACTIVE INFORMATION EXCHANGE SERVICE	7
3.3 TRANSACTIONAL SERVICE.....	7
4.0 SECURITY AND CONTROL OBJECTIVES	7
4.1 DATA CONFIDENTIALITY.....	8
4.2 SYSTEM AND DATA INTEGRITY.....	9
4.3 AUTHENTICATION AND NON-REPUDIATION.....	10
4.4 SYSTEM AVAILABILITY	10
4.5 CUSTOMER PROTECTION.....	11
5.0 SECURITY PRINCIPLES AND PRACTICES.....	13
5.1 HUMAN RESOURCE MANAGEMENT	13
5.2 FIREWALL INFRASTRUCTURE	14
5.3 SECURITY PRACTICES	15
6.0 RECOVERY AND BUSINESS CONTINUITY.....	17
7.0 OUTSOURCING MANAGEMENT	18
7.1 MANAGING OUTSOURCING RISKS	18
7.2 MONITORING OUTSOURCING ARRANGEMENTS.....	19
7.3 CONTINGENCY AND BUSINESS CONTINUITY PLANNING	19
8.0 BANK DISCLOSURE.....	19
9.0 CUSTOMER EDUCATION.....	20

1.0 INTRODUCTION

1.0.1 New and emerging technologies 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 exploit and rely increasingly on new technologies and the internet to operate their business and interact with the market, technology risks¹ will potentially increase, both for individual banks and the financial industry at large. In this new technology driven environment, it is critical that banks have flexible and responsive internal 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 prevalent and complex. The risk management process requires the board and management to decide on what and how much to invest in security and controls in computer systems, telecommunications and networks.

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

- a) identify, classify and assess risks that are relevant to the bank's operations.
- b) develop a documented plan containing policies, practices and procedures that address and control these risks.

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 inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities.

- c) implement and regularly test the plan.
- d) monitor risks and the effectiveness of the plan on an ongoing basis.
- e) update the plan periodically to take account of changes in technology, legal development and business environment including external and internal threats to information security.

1.0.6 The aim of this document 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 process.
- Strengthening system availability, security and recovery capability.
- Deploying strong cryptography and key management practices to protect customers' data.

1.0.7 All banks providing internet banking² must establish 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.

2.0 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 identification and assessment by going through the spectrum of relevant risks and carrying out impact analysis of the various risks on their business operations and systems. 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 Internet banking refers to the provision of banking services and products via electronic networks and delivery channels based on internet technologies, including web-based applications and wireless networks. 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.

2.0.2 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 financial, procedural and security controls are sound 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 destruction of information. Threat and vulnerability assessment findings would assist management in making decisions regarding the nature and extent of security controls required. Security awareness programmes should also be promulgated 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 software faults or hardware malfunction. A substantial task in disaster recovery planning is putting together a meaningful set 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 reinstate 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. The risk evaluation methodology can be divided into four parts: risk identification, risk analysis and quantification, risk treatment and risk monitoring.

2.1 Risk Identification

2.1.1 While the types of risks generated by internet banking services are not new, 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, operations and human elements.

2.1.2 During the risk identification process, consideration needs to be given to both the internet applications and the support 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 profile of the internet applications in a more comprehensive manner.

2.1.3 Some new types of threats as manifested in denial of service attacks have no precedents or equivalents in the physical world, but could cause severe disruption to the operations of a bank with consequential losses for all parties affected. Vigilant monitoring of these mutating, emerging risks is a crucial step in the risk containment exercise.

2.2 Risk Analysis and Quantification

2.2.1 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 Risk Treatment

2.3.1 Prior to analysing and treating risks, management must establish a risk classification methodology. For each type of material risks identified and analysed, management should develop and implement risk mitigation and control strategies that are consistent with the bank's information security requirements and its level of risk tolerance. Management must 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.

2.3.2 Banks must be 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 soundness 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. Conversely, it is also important that the bank does not offer a product or service on the internet if the necessary controls and security measures cannot be adequately implemented.

2.4 Risk Monitoring and Review

2.4.1 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. Routine testing and regular auditing of the

adequacy and effectiveness of the risk management process and the attendant controls and security measures taken should be conducted.

2.4.2 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 owned 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 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 according to 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 and the bank's internal systems may be exposed to 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 myriad remote locations.

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, spoofing, sniffing, hacking, mutating virus, worms and other forms of malicious or fraudulent acts pose heightened technology risk levels which banks would have rarely encountered before. It is imperative that banks implement strong security measures that can adequately address and control these types of risks and security threats. Banks must provide the assurance that transactions performed over the internet are adequately protected and authenticated.

This would require a security policy to be established to enable the following objectives to be met:

- Data confidentiality
- System and data integrity
- Authentication and non-repudiation
- System availability
- 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 encryption 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 process should be applied to communication sessions between the customers and the banks where confidentiality is required.

4.2 System and Data Integrity

4.2.1 System and data 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 which previously used to be only accessible from specified locations 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 may also want to install monitoring or surveillance systems that would alert them to any unusual or dubious online transactions taking place.

4.2.4 Factors that are pertinent to system and data integrity include:

- Logical access security³
- Physical access security⁴
- Processing and transmission controls⁵

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.

4.3 Authentication and Non-Repudiation

4.3.1 In internet banking, encryption technologies play an important role in ensuring confidentiality, authenticity and integrity. Customers are required to provide their user IDs and passwords so that their identity and authenticity could be verified before access to their accounts is permitted. In basic terms, the 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 security token, smart card or digital certificate).

4.3.2 Strong authentication can be achieved through the use of personal identification numbers, passwords, security tokens, biometrics and digital signatures. Customers also need to authenticate the bank's web site or online system which interacts with them through security mechanisms such as the secure sockets layer (SSL) server-authentication. Banks must ensure that encrypted and authenticated sessions remain intact throughout the duration of the communications. In the event of a security lapse, the session must be terminated and the affected transactions nullified.

4.3.3 For some systems and certain types of transactions, capturing the attribute of non-repudiation in the form of digital signature, collision-free hash value of the entire transaction or unique authorisation code may become necessary. This provides conclusive proof of participation by both the sender and receiver in an online transaction environment. Public key encryption, digital signature and Certification Authority⁶ (CA) arrangements can be used to impart an enhanced level of security, authentication and authorisation. They can uniquely identify the person who initiates a transaction, append a digital signature to the transaction, detect unauthorised modifications and prevent disavowal of the transaction.

4.4 System Availability

4.4.1 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

⁶ A Certification Authority is a trusted third party which enrolls, validates and authenticates the identities of users or account holders. The authentication process generally involves the issuance and administration of digital certificates.

services expect to be able to access the online systems 24 hours every day of the year, meaning near zero system downtime.

4.4.2 Key considerations 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.

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

4.4.4 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.

4.4.5 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.

4.5 Customer Protection

4.5.1 Customer protection is of paramount importance in internet banking. The bank must ensure that a customer is properly identified and authenticated before access to online banking functions is permitted.

4.5.2 Banks should advise customers on how to select or create robust passwords, personal identification numbers and authorisation codes that cannot be easily guessed or derived. For applications which require stronger authentication than UID/PIN, enhanced methods based on security tokens, smartcards and biometric devices should be deployed.

4.5.3 Strong cryptography such as DES-168, AES-128/192/256, SSL/RC4-128, RSA-1024, IDEA-128, ECC-163 bit encryption should be used to protect and authenticate communication sessions between the customer and the bank. The strength of cryptography depends largely on the size of the cipher key. Constant advances in computer hardware, computational number theory and cryptanalysis will compel larger key lengths to be used in future. Some contemporary cipher algorithms will have to be replaced when they lose their potency in the face of ever increasing computer speed and power.

4.5.4 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. Specific online confirmatory authorisation for each transaction above a pre-set value could be imposed by the bank to fortify transactional security. The additive use of digital certificates to strengthen the authentication process can also be introduced. Digital certificates are capable of making access control more secure and easier to manage than traditional password schemes. Mutual authentication between the customer and the bank could be made through the exchange and verification of digital certificates.

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 trojan horses, backdoor programs, 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 distribution 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.

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 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 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. These functions include systems initialisation, network security configuration, access control system installation, changing operating system parameters, firewall implementation, modifying contingency plans, invoking emergency procedures, obtaining access to backup recovery resources and 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, security 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 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 attacks or sabotage by trusted employees are potentially among the most serious risks that a bank faces. 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.

5.1.4 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.

5.2 Firewall Infrastructure

5.2.1 Firewalls are key components of secure networks which are needed to separate the internal network segments from the internet. Internal and external networks operating at varying sensitivity and protection levels should be isolated from one another by appropriate firewall configurations and architecture.

5.2.2 Generally, the internal and external networks must be physically and logically isolated from each other by firewalls. Where possible, all incoming and outgoing traffic should be subject to filtering and scrutiny. A common fault is to allow dial-up connections to the internet behind corporate firewalls. These back-door connections invariably cause serious security exposures in networks.

5.2.3 To ensure effectiveness, all firewall configurations should be subject to thorough testing and evaluation for vulnerabilities or loopholes prior to being put into production. An independent security expert should be engaged at least annually to carry out a comprehensive review and analysis of network vulnerability and recovery preparedness. Assessment, configuration and enhancement of firewalls, proxy servers and filtering routers on an ongoing basis are often complex tasks which require internal or external expertise.

5.2.4 Packet-filtering firewalls should be supplemented by application level security in order to reduce attack severity at the network protocol level. This would include service restrictions in servers to only those which are essential. The server systems software should be updated on a regular basis to patch up security deficiencies that may be discovered from time to time. Network and host based intrusion detection systems and denial of service filters can also be used in front-line servers as well as inside firewalls to protect critical assets within the network. Application based filters to strip Java, ActiveX, applets and other executable files, programs, codes or attachments may also be applied.

5.3 Security Practices

5.3.1 Banks should take the following actions relating to security practices:

- a) Deploy secure operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of enhancements, updates and patches recommended by system vendors.
- b) Change all default passwords for new systems immediately upon installation as they provide the most common means for intruders to break into systems.

- c) Install firewalls between internal and external networks as well as between geographically separate sites.
- d) Develop built-in redundancies for single points of failure which can bring down the entire network.
- e) Engage independent security specialists 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.
- f) Conduct penetration testing at least annually.
- g) Use network scanners, intrusion detectors and security alerts.
- h) Implement anti-virus software.
- i) Establish security monitoring procedures.
- j) Maintain access security logs and audit trails.
- k) Analyse security logs for suspicious traffic and access attempts.
- l) Establish an incident management and response plan.
- m) Test the predetermined action plan relating to security incidents.
- n) Install network analysers which can assist in determining the nature of an attack and help in containing such an attack.
- o) Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.
- p) Maintain a rapid recovery capability.
- q) Conduct security awareness education and programs.
- r) Require frequent audits to be conducted by security professionals or internal auditors who have the requisite skills.
- s) Consider taking insurance cover for various insurable risks, including recovery and restitution costs.

6.0 RECOVERY AND BUSINESS CONTINUITY

6.0.1 As no computer system is impregnable and its security completely foolproof, 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 the business, network, system and operating environment occur.

6.0.2 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. Hotsite recovery capability must be created and maintained if the bank's primary delivery channels rely predominantly on the internet. 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 continue to service customers.

6.0.3 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.

6.0.4 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.

6.0.5 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.

6.0.6 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.

7.0 OUTSOURCING MANAGEMENT

7.0.1 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).

7.0.2 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.

7.1 Managing Outsourcing Risks

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.2 Monitoring Outsourcing Arrangements

7.2.1 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.

7.2.2 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.

7.3 Contingency and Business Continuity Planning

7.3.1 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.

7.3.2 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 to continue operations or render the services required. It should incorporate identification of viable alternatives for resuming its internet banking operations elsewhere.

8.0 BANK DISCLOSURE

8.0.1 The bank should provide clear information to 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.

8.0.2 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.

8.0.3 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.

9.0 CUSTOMER EDUCATION

9.0.1 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 functions connected with the operation of their banking accounts and transaction services.

9.0.2 Customer education may include web-based online education or other media whereby a guided learning experience may be defined. When new operating features or requirements, particularly those relating to security, integrity and authentication, are being introduced, the bank should ensure that customers have sufficient instructions 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 actions in reporting security problems.

9.0.3 To raise security awareness, banks should exhort customers on the need to protect their personal identification numbers, passwords, personal details and other confidential data. The following advice would be instructive in helping customers to compose robust PINs and take on better security measures:

- PIN should be at least 6 characters in length.
- PIN should be a permutation of letters and numbers that is not found in dictionaries nor easily linked to the user.
- PIN should not be based on user log-on names, family names, birthdays, personal telephone numbers or other associative data.
- PIN must be kept confidential at all times and not be divulged to anyone.
- PIN must be memorised and not stored in computer hard-disk, diskette or other insecure devices.
- Browsers and application software should be upgraded to support SSL128-bit encryption or a higher encryption standard.
- 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.

Access to PIN security instructions and information should be displayed prominently in the user log-on or PIN entry web page. This notification and related information should be provided in a friendly and easily locatable manner and not be obscured or embedded in other data.

Note:

For the purpose of this document, the words "should", "must", "required to", "need to" and "has to" signify mandatory requirements.