CONSULTATION PAPER

P012 - 2012

JUNE 2012

TECHNOLOGY RISK MANAGEMENT GUIDELINES

MAS

Monetary Authority of Singapore

PREFACE

The MAS Internet Banking and Technology Risk Management Guidelines have been updated to enhance financial institutions' oversight of technology risk management and security practices. The new guidelines include guidance on existing and emerging technology trends and security concerns in the financial industry. In addition, the circulars on IT outsourcing, endpoint security and data protection, information systems reliability, resiliency and recoverability have been amalgamated into the guidelines to facilitate ease of reference by users. The name of the new guidelines has been changed to "Technology Risk Management Guidelines".

MAS invites interested parties to submit their views and comments on the following areas in the new guidelines, where additions and significant changes have been made:

a) Data Centres Protection and Controls
Financial institutions' critical data, applications, systems and network devices are maintained in data centres. Chapter 10 provides guidance on the scope of assessment which financial institutions should perform to identify security and operational weaknesses in their data centres. This section also describes measures which should be implemented so that data centres are resilient and physically secured against internal and external sabotage.

b) Mobile Banking and Payment Security
Mobile banking and payments are extensions of online financial services and payments on mobile devices. Whilst mobile banking and payments face similar threats as those of internet banking and payments, Section 12.2 covers specific risks confronting the mobile security landscape and the importance of educating customers on security measures to protect their mobile devices from theft and loss as well as viruses and other malicious software.

c) Payment Card System and ATM Security
Financial institutions, providing payment card services, should institute various measures to combat the increase in payment card fraud. Chapter 13 covers a suite of measures that should be adopted to enhance the security of payments cards, card acceptance terminals and processing

systems, as well as guidance on fraud detection mechanisms. This section also recommends certain detective measures that financial institutions should take to mitigate this threat.

d) Combating Cyber Threats
A multi-layered security strategy should be implemented to protect financial systems offered via the internet platform. Appendix E addresses security measures for online systems. In particular, to address man-in-the-middle attack (MITMA), financial institutions are advised to implement transaction-signing for high risk transactions (e.g. payments, fund transfer limits or changes to personal details) performed by customers.

e) Customer Protection and Education
Customer protection and education requirements are updated in Appendix F to include new guidance for financial institutions to protect customers' login credentials for online systems. Financial institutions are also advised to educate customers on features and risks of different payment cards as well as measures to secure their cards.

Electronic submission is encouraged. Please submit your comments by 16 July 2012 to:

Technology Risk Supervision Division
Specialist Risk Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Email: techrisk@mas.gov.sg
Fax: 62299659

Please note that any submission received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

TABLE OF CONTENTS

1 INTRODUCTION

1.0.1 The advancement of information technology (IT) has brought upon rapid changes to the way businesses, systems and operations are being conducted in the financial industry. IT is no longer a support function within a financial institution[1] (FI) but a key enabler to business in reaching and supporting customers, local or overseas.

1.0.2 Financial systems and networks supporting FIs' business operations have also grown in scope and complexity over the years. FIs offering a diversity of products and services could have their financial systems operating in multiple locations and supported by different service providers.

1.0.3 FIs are faced with the challenge of keeping pace with the needs, preferences and habits of consumers who are getting more IT-savvy and switching to internet and mobile devices for financial services, given their speed, convenience and ease of use. Increasingly, FIs are deploying more advanced technology and online systems, including internet banking systems, mobile banking and payments, online trading platforms and insurance portals, to reach their customers. In this regard, FIs should fully understand the magnitude and intensification of technology risks from these systems. They should also put in place adequate and robust risk management systems as well as operating processes to manage these risks.

[1] "Financial Institution" has the same meaning as in section 27A(6) of the Monetary Authority of Singapore Act (Cap. 186).

1.0.4 Guidelines set out sound risk management principles or best practice standards to govern the conduct of the financial institutions. Specifically, the Technology Risk Management Guidelines seek to guide the financial institutions in the following:

- establishing a sound and robust technology risk management framework;
- Strengthening system security, reliability, resiliency, availability and recoverability; and
- Deploying dynamic authentication to protect customer data, transactions and systems. While contravention of the guidelines is not a criminal offence and does not attract civil penalties, the degree of observance with the spirit of the guidelines by an institution will impact MAS' overall risk assessment of that institution.

2 APPLICABILITY OF THESE GUIDELINES

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

2.0.2 The objective of these guidelines is to promote the adoption of sound processes in managing technology risks and the implementation of security practices in regulated FIs. 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 FIs. Each FI can expect that MAS will take a keen interest as to how and the extent to which it has implemented these guidelines.

3 OVERSIGHT OF TECHNOLOGY RISKS BY BOARD AND SENIOR MANAGEMENT

3.0.1 IT is a core function of many FIs. When core systems fail and customers cannot access their accounts, an FI's business operations may immediately come to a standstill. The impact on customers is instantaneous and the consequences are widespread.

3.0.2 In view of the importance of the IT function in supporting an FI's businesses, critical or key IT decisions should not be made by IT professionals only. The board of directors and senior management should be involved in the IT decision-making process to ensure that IT is capable of supporting the organisation's strategies and objectives, as well as to ensure adequate oversight of technology risks within the organisation.

3.1 Roles and Responsibilities

3.1.1 The responsibility and accountability of the board and senior management is a basic tenet of sound practices and good corporate governance.

3.1.2 The board of directors and senior management are fully responsible and accountable for managing technology risks, which are becoming increasingly complex, dynamic and pervasive.

3.1.3 They are also fully responsible for the implementation of effective internal controls and risk management practices to achieve robustness, reliability, resiliency and recoverability of IT systems and infrastructures.

3.1.4 The board and senior management should review and appraise the cost-benefit issues regarding investment in controls and security measures for computer systems, networks, data centres, operations and backup facilities. Factors such as reputation, customer confidence, consequential impact and legal implications should be evaluated, in addition to cost considerations.

3.2 IT Policies, Standards and Procedures

3.2.1 IT policies, standards and procedures are critical components of the framework to manage technology risks. They should stipulate the parties responsible, objectives of and processes for safeguarding information assets in the organisation.

3.2.2 Due to rapid changes in the IT operating and security environment, policies, standards and procedures should be regularly reviewed and updated so that they remain current and relevant.

3.2.3 Compliance and enforcement processes should be implemented to verify that IT requirements are met. Follow-up processes should be implemented so that compliance deviations are addressed and remedied on a timely basis.

3.3 People Selection Process

3.3.1 Careful selection of people is crucial in minimising technology risks due to system failure, internal sabotage or fraud. As people play an important role in managing systems and processes in an IT environment, the FI should implement an employee screening process that is comprehensive and effective.

3.3.2 Protection of customer information should be imposed and maintained by staff, vendors and contractors, who are authorised to access an FI's critical systems, network, data and computer resources.

3.4 IT Security Awareness

3.4.1 A comprehensive IT security awareness training program should be established to enhance the overall IT security awareness level in the organisation. The program should include information on IT security policies and standards as well as individual responsibility in respect of IT security and measures that should be taken to safeguard information assets. Every staff in the organisation should be made aware of the Computer Misuse Act and other applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to IT resources.

3.4.2 The program should be conducted and updated at least annually and extended to all new and existing employees, contractors and vendors who have access to an FI's IT resources and systems.

3.4.3 The program should be supported by senior management, and reviewed regularly to ensure that the contents of the program remain current and relevant, taking into consideration the evolving nature of technology as well as emerging risks and threats.

4 TECHNOLOGY RISK MANAGEMENT FRAMEWORK

4.0.1 A sound and robust technology risk management framework requires the board and senior management to be responsible and accountable for managing and controlling technology risks.

4.0.2 A technology risk management framework should be established to manage technology risks in a systematic and consistent manner. The framework should encompass the following attributes:

a. Roles and responsibilities of the technology risk management process;

b. Identification and prioritisation of information assets;

c. Identification and assessment of impact of anticipated known and emerging threats, risks and vulnerabilities;

d. Implementation and follow-up of appropriate controls to mitigate unacceptable risk levels; and

e. Periodic update and monitoring of risk assessment to include changes in systems, environmental or operating conditions that would affect risk analysis.

4.0.3 Effective risk management practices and internal controls should be instituted to achieve data confidentiality[2], system integrity[3] and availability[4] in the organisation. In addition, appropriate measures should be implemented to protect customer data, which are stored and processed in systems. Customers should be properly identified and authenticated before access to sensitive customer information or online transaction functions are permitted. Sensitive customer information including login credentials, passwords and PINs should be secured against exploits such as ATM skimming, card cloning, hacking, phishing and malware.

[2] Data confidentiality refers to the protection of sensitive information such as customer data from unauthorised access.

[3] System integrity refers to the accuracy, reliability and completeness of information processed, stored or transmitted between FIs and customers.

[4] System availability refers to the accessibility and uptime performance of systems for carrying out business operations and serving customer requirements.

4.1 Risk Management Process

4.1.1 Information system assets[5] should be adequately protected from unauthorised access, deliberate misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure. Risks that are deemed material to an FI should be thoroughly evaluated and prioritised to enable a strategy to be developed for addressing and mitigating these risks.

4.1.2 A comprehensive IT security strategy should be developed. This is a vital component of an effective risk management process and should have the support of the highest echelon of management.

4.1.3 The risk management process should include the identification, measurement and assessment of risks, as well as formulating a plan to mitigate risks down to an acceptable level.

4.1.4 An identification of the list of information system assets that need to be protected should be performed. The value of information system assets should be ascertained to facilitate the ranking and prioritisation of these assets. At the same time, it is essential to have a clear policy commitment to asset protection with respect to its security goals. Different types of systems would have different values to an FI, depending on their impact on the organisation if there were a loss of systems confidentiality, integrity and availability arising from attacks, vulnerability exploitation or adverse incidents

4.2 Risk Identification

4.2.1 Risk identification entails the determination of the threats and vulnerabilities to the FI's IT environment which comprises the internal and external networks, hardware, software, applications, systems interfaces, operations and human elements.

4.2.2 A threat can be defined as any condition, circumstance, incident or person with the potential to cause harm by exploiting 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

4.2.3 Security threats such as those manifested in denial of service attacks, internal sabotage and malware infestation could cause severe harm and disruption to

[5] Information systems assets refer to data, systems, networks, devices and equipment.

the operations of an FI with consequential losses for all parties affected. Vigilant monitoring and identification of such mutating and growing risks is a crucial step in the risk containment exercise.

4.3 Risk Assessment

4.3.1 Following the task of risk identification, an analysis and quantification of the potential impact and consequences of these risks on the overall business and operations should be performed. With this analysis, management will be able to prioritise the risks, and perform the cost-benefit analysis for risk mitigation actions.

4.3.2 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 occur.

4.3.3 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.

4.4 Risk Treatment

4.4.1 For each type of risk identified and analysed, an FI should develop and implement risk remediation and control strategies that are consistent with the value of the information asset and the level of risk tolerance.

4.4.2 Risk mitigation entails a methodical approach for evaluating, prioritising and implementing appropriate risk-reduction controls, which includes security measures. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks.

4.4.3 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 assess its risk tolerance for damages and losses in the event that a given risk-related event materialises. The costs of risk controls should be balanced against the benefits to be derived.

4.4.4 It is imperative that an FI is able to manage and control risks in a manner that would allow it the capacity to absorb losses that may eventuate without jeopardising its financial and operational viability and stability. When deciding on the adoption of alternative controls and security measures, management should also be conscious of its costs and effectiveness in respect of the risks being mitigated.

4.4.5 Where the threats to the safety and soundness of the system are insurmountable and the risks cannot be adequately controlled, an FI should refrain from implementing and running such a precarious system.

4.4.6 As a risk mitigating measure, an FI could consider taking insurance cover for various insurable risks, including recovery and restitution costs.

4.5 Risk Monitoring and Reporting

4.5.1 A risk register which facilitates the monitoring and reporting of risks should be maintained. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. The risk register should be updated periodically. A monitoring and review process should also be instituted for continuous assessment and treatment of risks.

4.5.2 To facilitate risk reporting to management, IT risk metrics should be developed to highlight systems, processes or infrastructure that have the highest risk exposure. An overall technology risk profile of the organisation should also be provided to the board and senior management. In addition, risk events, regulatory requirements and audit observations should be considered in determining the IT risk metrics.

4.5.3 In view of changes in IT environment and delivery channels, risk parameters may change. Thus, the risk processes should be reviewed and enhanced accordingly. Re-evaluation of past risk-control methods with renewed testing and assessment of the adequacy and effectiveness of risk management processes should be conducted.

4.5.4 Management should review and update its risk control and mitigation approach, taking into account changing circumstances and variations in its risk profile.

5 MANAGEMENT OF IT OUTSOURCING RISKS

5.0.1 Outsourcing comes in many forms and permutations. Some of the most common types of outsourcing are in IT and business processing functions ranging from systems development, maintenance and support to data centre operations, network administration, disaster recovery services, application hosting and cloud computing. These activities can involve the provision of IT capabilities and facilities by a single third party or multiple vendors located in Singapore or abroad.

5.0.2 The responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the FI, its board and senior management. The FI should put in place a proper framework, policies and procedures to evaluate, approve, review, control and monitor the risks of all its outsourcing activities.

5.1 Due Diligence

5.1.1 The board and senior management must fully understand risks associated with IT outsourcing. Before a service provider is appointed, due diligence should be carried out to determine its viability, capability, reliability, track record and financial position.

5.1.2 The contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties should be carefully and properly defined in written agreements. The requirements and conditions 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.

5.1.3 The service provider should be required to provide access to all parties nominated by the FI 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 to carry out inspections, supervisions or examinations of the service provider's roles, responsibilities, obligations, functions, systems and facilities must be explicitly documented in the agreements.

5.1.4 Contracts and arrangements with the service provider, as well as management of outsourced functions, 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.

5.1.5 Outsourcing in any configuration or at any location should not result in any weakening or degradation of the FI's internal controls. The FI should require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive information, such as customer data, computer files, records, object programs and source codes.

5.1.6 The service provider should implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations.

5.1.7 The security practices and processes of the service provider should be monitored and reviewed on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations and services provided by the service provider.

5.1.8 A process of monitoring service delivery, performance reliability, processing capacity and security enforcement should also be established for the purpose of gauging ongoing compliance with agreed service levels and the viability of its operations. Monitoring metrics and reports specific to the FI's outsourced function should be provided to the FI.

5.1.9 A Threat and Vulnerability Risk Assessment (TVRA) of the service provider's data centre should be performed on a periodic basis, including penetration testing. The purpose of the TVRA is to identify security and operational weaknesses pertaining to the data centre in order to determine the level and type of protection that should be established to safeguard it. The FI should also require the service provider to have a remediation plan to address all identified issues within a reasonable timeframe.

5.1.10 Senior management should require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

5.1.11 As human error still accounts for the bulk of systems downtime and failures, all parties and personnel concerned, including those from service provider, should receive regular training in activating the contingency plan and executing recovery procedures.

5.1.12 The disaster recovery plan should be reviewed, updated and tested regularly in accordance with changing technology conditions and operational requirements.

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

5.1.14 As part of the due diligence process, onsite visits to the service provider's data centres hosting outsourced data and / or applications should be performed to assess the quality of operation and security controls at these data centres.

5.2 Cloud Computing

5.2.1 Cloud computing is a service and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (servers, storage and services). Users of such services may not know the exact locations of servers, applications or data, within the service provider's computing infrastructure that were hosting, storing or processing information for them.

5.2.2 Besides performing its due diligence for all forms of outsourcing arrangements, an FI should be aware of unique attributes and risks especially in areas of data integrity, sovereignty commingling, platform multi-tenancy, recoverability and confidentiality as well as legal issues such as regulatory compliance, auditing and data offshoring.

5.2.3 As cloud computing service providers adopt multi-tenancy and data commingling architectures in order to process data for multiple customers, the FI should pay attention to these service providers' abilities to isolate and clearly identify its customer data and other information system assets for protection.

5.2.4 In the event of contract termination with the service provider, either on expiry or prematurely, the FI should have the contractual power and means to have all such IT information and assets promptly removed or destroyed at the service provider's systems and backups.

5.2.5 The service provider's ability to recover the outsourced systems and IT services within the stipulated recovery time objective should also be verified prior to the outsourcing arrangement.

6 ACQUISITION AND DEVELOPMENT OF INFORMATION SYSTEMS

6.0.1 Many systems fail because of poor system design and implementation, as well as inadequate testing. System deficiencies and defects should be identified early at the system design, development or testing phases.

6.0.2 For major projects, a steering committee, consisting of business owners, various management, development and other stakeholders should be established to provide oversight and monitoring of the progress of the project, including deliverables to be realised at each phase of the project and milestones to be reached according to the project timetable.

6.1 IT Project Management

6.1.1 In a project management framework, tasks and processes for developing or acquiring new systems should include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables. Roles and responsibilities of personnel involving in the project should also be clearly defined.

6.1.2 A project plan should be clearly documented. Deliverables to be realised at each phase of the project as well as milestones to be reached should also be determined and documented.

6.1.3 User functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans and service performance expectation should be approved at appropriate management levels. Adequate documentation for these areas should be maintained.

6.1.4 Management oversight of the project should be established to ensure milestones are reached and deliverables are realised in a timely manner. Issues or problems which could not be resolved at the project committee level should be escalated to senior management for attention and intervention.

6.2 Security Requirements and Testing

6.2.1 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 in the early phase of system development or acquisition. A compliance check against the FI's security standards and regulatory requirements should be performed.

6.2.2 A methodology approved by senior management should set out how and what system testing[6] should be conducted. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

6.2.3 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 users whose systems and operations are affected by the new changes. (Refer to Appendix A for details on Systems Security Testing and Source Code Review.)

6.2.4 Penetration testing should be conducted prior to the commissioning of a new system which offers internet accessibility and open network interfaces. Vulnerability scanning of external and internal network components that support the new system should also be performed. Vulnerability scanning should be conducted at least quarterly with penetration testing at least yearly.

6.2.5 Separate physical or logical environments for unit, integration, system and user acceptance testing (UAT) should be maintained. Vendor and developer access to UAT environment should be strictly monitored.

6.3 Source Code Review

6.3.1 There are different ways of coding programs which may conceal security threats and loopholes, deliberate or unintentional. System and user acceptance testings are ineffective in detecting malicious codes, trojans, backdoors, logic bombs and other malware. Black-box testing is not an effective tool in identifying or detecting these security threats and weaknesses.

6.3.2 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

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

development stage and have them fixed before the system is implemented. Concurrently, code quality and programming practices can also be improved.

6.3.3 A high degree of system and data integrity is required for all systems. FIs should exercise due diligence in ensuring its applications have appropriate security controls, taking into consideration the type and complexity of services these applications provide.

6.3.4 Based on the FI's risk analysis, specific application modules and 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.

6.4 End User Development

6.4.1 There are common business application tools and software which allow business users to develop simple programs to automate their operations, perform data analysis and generate reports for the organisation and customers.

6.4.2 User access and data protection controls, at minimum, should be implemented in these applications.

6.4.3 End user developed program codes, scripts and macros should also be reviewed and tested before distribution to safeguard the integrity and reliability of the application functionalities as well as the data which is processed.

6.4.4 Business impact analysis should also be performed to assess the importance of these programs to business. Recovery measures should be implemented for programs which are important to the business.

7 IT SERVICE MANAGEMENT

7.0.1 Critical business functions rely on technology and complex IT systems to automate and support its daily operations. A robust IT service management framework is essential for supporting IT systems, services and operations, managing changes, incidents and problems as well as ensuring the stability of the production IT environment. The framework should comprise the governance structure, processes and procedures for change management, software release management, incident and problem management as well as capacity management.

7.1 Change Management

7.1.1 A change management process should be established to ensure that changes to production systems are assessed, approved, implemented and reviewed in a controlled manner.

7.1.2 The change management process should be applied to changes pertaining to system and security configurations, patches for hardware devices and software updates.

7.1.3 Prior to deploying changes to the production environment, a risk and impact analysis of the change request should be performed in relation to existing infrastructure, network, up-stream and downstream systems. The FI should also determine if the introduced change would spawn security implications or software compatibility problems to affected systems or applications.

7.1.4 The impending change should be adequately tested and accepted by users prior to its migration to production system. The FI should develop and document appropriate test plans for the change. Test results with user sign-offs should be obtained prior to the migration.

7.1.5 All changes to the production environment should be approved by parties delegated with the authority.

7.1.6 To minimise risks associated with changes, FIs should perform backups of affected systems or applications prior to the change. A rollback plan should be established to allow an FI to revert to former version if a problem is encountered during or after the deployment. If the change does not allow the FI to revert to a prior status, alternative recovery options in the event that the change is not implemented successfully in the production environment should be explored.

7.1.7 Audit and security logs are useful information which facilitates investigations and trouble shooting. It is important that the logging facility is enabled to record activities that are performed during the migration process.

7.2 Program Migration

7.2.1 Program migration involves the movement of software codes and scripts from development environment to test and production environments. Unauthorised and malicious codes which are injected during migration process could compromise data, systems and processes in the production environment.

7.2.2 Separate physical or logical environments for systems development, testing, staging and production should be provided; only production environment should be connected to the internet.

7.2.3 Segregation of duties should be enforced so that no single individual has the ability to develop, compile and move object codes from one environment to another.

7.2.4 After a change has been successfully implemented in the production environment, the change should also be replicated and migrated to disaster recovery systems or applications for consistency.

7.3 Incident and Security Incident Management

7.3.1 An incident occurs when there is an unexpected disruption to the standard delivery of IT services. Incidents should be appropriately managed within an organisation to avoid the situation of mishandling that result in a disruption of IT services.

7.3.2 An incident management framework should be established with the objective of restoring normal IT service as quickly as possible following the incident, and with minimal impact to the business operations. The framework should define the process for recording, analysing, remediating and monitoring incidents. The roles and responsibilities of staff involved in the incident management process should also be established.

7.3.3 An FI may delegate the responsibility of incident severity assignment to a centralised technical helpdesk function. It is important that incidents are accorded with the appropriate severity level at the start. Helpdesk staff should be trained to discern incidents of high severity level. In addition, criteria used for assessing severity levels of incidents should be established and documented.

7.3.4 Depending on the severity level, corresponding escalation procedures and resolution timeframe should be established to ensure that incidents are addressed in a timely manner.

7.3.5 For security incidents[7], the predetermined escalation and response plan is tested on a regular basis.

7.3.6 A computer emergency response team, comprising personnel with necessary technical and operational skills should be formed and assembled when required, to handle major incidents.

7.3.7 In some situations, major incidents may further develop unfavourably into a crisis. Senior management should be kept apprised of the development of these incidents so that the decision to activate disaster recovery plan could be made on a timely basis.

7.3.8 As part of incident reporting process, FIs should notify MAS of incidents which result in the widespread unavailability of online financial services[8]. Security incidents involving hacking or intrusion offences should also be reported to MAS and the relevant law enforcement agencies. The notification should be made within thirty (30) minutes upon the occurrence of the event.

7.3.9 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 FIs. FIs should include in their incident response procedures a predetermined action plan to address public relations issues.

7.3.10 Public announcement of major incident which warrants disclosure to affected customers should be made on a timely basis. The announcement should include a chronological description of events which trigger the incident, its impact as well as measures taken to address and prevent the incident from happening again.

7.3.11 As incidents may stem from numerous factors, FIs should perform a root-cause and impact analysis for major incidents which result in severe disruption of IT services. Remediation actions should be taken to prevent the recurrence of similar incidents.

7.3.12 For security incidents and major incidents, FIs should submit a root-cause and impact analysis report to MAS within one (1) month upon the occurrence of these incidents. The report should contain an executive summary of the

[7] Examples of security incidents include virus outbreak, malware infiltration, systems hacking, account impersonation or compromise, phishing attack, internal sabotage or denial of service attacks.

[8] Online financial services refer to the provision of banking, trading, insurance or other financial 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.

incident, an analysis of root causes which trigger the event, its impact as well as measures taken to address the consequences of the event.

7.3.13 The root-cause and impact analysis report should encompass the following areas:

a. Root Cause Analysis

   i. When did it happen?

   ii. Where did it happen (systems, network, database, locations etc)?

   iii. Why and how did the incident happen?

   iv. What caused the error?

   v. Was this a recurrent incident? If yes, how often had this occurred over the last 3 years?

   vi. What lessons were learnt from this incident?

b. Impact Analysis

   i. Extent, duration or scope of the incident (what systems, resources, customers etc were affected);

   ii. Magnitude of the incident in terms of forgone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation & confidence etc); and

   iii. Breach of regulatory guidelines and conditions as a result of the incident.

c. Corrective and Preventive Measures

   i. Immediate corrective action to be taken to address consequences of the incident. Priority should be placed on addressing customers' concerns and / or compensation;

   ii. Measures to address the root cause of the incident; and

   iii. Measures to prevent similar or related incidents from occurring.

7.3.14 All incidents should be monitored and tracked to closure. Incidents should be addressed adequately within corresponding resolution timeframes.

7.4 Problem Management

7.4.1 A problem stems from the unknown cause of one or more incidents of similar nature. While the objective of incident management is to restore the IT service as soon as possible upon the occurrence of an IT disruption, the objective of problem management is to determine and eliminate the root cause to prevent the occurrence of repeated problems.

7.4.2 Clear roles and responsibilities of staff involved in the problem management process should be established. Problems should be identified, classified, prioritised and addressed in a timely manner.

7.4.3 To facilitate the classification process, criteria that are used to categorise problems into respective severity levels should be clearly defined. To effectively monitor and escalate protracted problems, target resolution or response time as well as appropriate escalation process for each severity level should be established.

7.4.4 Besides responding to problems as they occur, a proactive approach should be adopted to identify issues and potential risks before such issues evolve to be problematic. A quarterly trend analysis of past incidents should be performed to facilitate the identification and rectification of potential problems.

8 SYSTEMS RELIABILITY, AVAILABILITY AND RECOVERABILITY

8.0.1 The reliability, availability, and recoverability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in the operational and functional capabilities of an FI. When mission-critical systems fail, the disruptive impact on the FI's operations and functions will usually be immediate, severe and widespread, with serious consequences to reputation.

8.0.2 As all systems are vulnerable, FIs should define their recovery and business resumption priorities. Contingency procedures should be tested and practised so that business and operating disruption arising from a serious incident could be minimised.

8.1 System Availability

8.1.1 Important factors associated with maintaining high system availability are adequate capacity, reliable performance, fast response time, scalability and swift recovery capability.

8.1.2 FIs may employ a number of complex interdependent system and network components for their IT processing. An entire system can become inoperable when a single critical hardware component or software module malfunctions or damaged. FIs should develop built-in redundancies for single points of failure which can bring down the entire network. Standby hardware, software and network components that are necessary for fast recovery should be maintained.

8.1.3 FIs should achieve a near zero system downtime[9] for critical systems.

8.2 Disaster Recovery Plan

8.2.1 In formulating and constructing a rapid recovery plan, scenario analysis should be included to identify and address various types of contingency scenarios. Scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary data centre should be considered.

[9] Other than during periods of planned maintenance, institutions should enhance their system and infrastructure resiliency and deploy active-active configuration for these systems to minimise downtime.

8.2.2 To strengthen recovery measures relating to large scale disruptions and to achieve risk diversification, rapid operational and backup capabilities at the individual system or application cluster level should be implemented. Inter-dependencies between critical systems should be considered in the recovery plan and contingency tests.

8.2.3 Recovery and business resumption priorities must be defined accordingly. Specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) should be established for systems and applications.

8.2.4 RTO refers to the required time taken to recover an IT system from the point of disruption. RPO refers to the acceptable amount of data loss for an IT system should a disaster occur.

8.2.5 For critical systems, a RTO of four hours or less should be established and maintained.

8.2.6 Stringent RPOs that are commensurate with the FI's business requirements should also be defined.

8.2.7 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.

8.2.8 The required speed of recovery will depend on the criticality of resuming business operations, the type of services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers. Recovery strategies and technologies such as on-site redundancy and real-time data replication could be explored to enhance the FI's recovery capability.

8.2.9 FIs which outsource critical systems to offshore service providers are heavily dependent on the stability and availability of cross-border network links. To minimise impact to business operations in the event of a disruption (e.g. due to earthquake), cross-border network redundancy with strategies such as engagement of different network service providers and alternate network paths should be instituted.

8.2.10 High severity incidents if handled inappropriately may result in disastrous situations. The recovery plan and incident response procedures should be evaluated annually and updated as and when changes to business operations, systems and networks occur.

8.3 Disaster Recovery Testing

8.3.1 During a system outage, an FI 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.

8.3.2 The effectiveness of recovery requirements and the ability of an FI's staff in executing or following the necessary emergency and recovery procedures should be tested and validated at least annually.

8.3.3 Various scenarios which include total shutdown or incapacitation of the primary computer site as well as component failure at the individual system or application cluster level should be included in disaster recovery tests.

8.3.4 Inter-dependencies between critical systems should be included in the tests. FIs, where their networks and systems were linked to specific service providers and vendors, should conduct bilateral or multilateral recovery testing.

8.3.5 Business users should be involved in the design and execution of comprehensive test cases so as to obtain assurance that recovered systems function accordingly. FIs should also participate in disaster recovery tests of systems hosted overseas.

8.4 Data Backup Management

8.4.1 A data backup strategy, to store critical information on a regular basis for recovery purpose, should be developed.

8.4.2 As part of data backup and recovery strategy, FIs may implement specific data storage architectures such as Direct-Attached Storage (DAS), Network-Attached Storage (NAS) or Storage Area Network (SAN) sub-systems connected to production servers. In this regard, FIs are required to review the architecture and connectivity of sub disk storage systems for single points of failure and fragility in functional design and specifications, as well as technical support by service providers. (Refer to Appendix B for details on Storage System Resiliency.)

8.4.3 Periodic testing and validation of the recovery capability of backup media should be carried out and assessed for adequacy and effectiveness.

8.4.4 Backup tapes and disks containing sensitive data should be encrypted before they are transported offsite for storage.

9 OPERATIONAL INFRASTRUCTURE SECURITY MANAGEMENT

9.0.1 The IT landscape is fraught with security threats such as denial of service attacks, spamming, spoofing, sniffing, hacking, keylogging, phishing, middleman interception, mutating virus, worms and other forms of malware with increasing frequency and malignancy. It is imperative that FIs implement security solutions at the data, application, database, systems and network layers to adequately address and contain these threats.

9.1 Data Loss Prevention

9.1.1 Internal sabotage, clandestine espionage or furtive attacks by trusted employees, contractors and vendors are potentially among the most serious risks that FIs could face in an increasingly complex and dynamic IT environment. Current and past employees, contractors, vendors and those who have an intimate knowledge of the inner workings of the FI's systems, operations and internal controls have a significant advantage over external attackers. A successful attack not only jeopardises customer confidence in the FI's internal control systems and processes but also causes real financial loss when trade secrets and proprietary information are divulged. FIs should identify important information assets and adopt adequate measures to detect and prevent unauthorised access, copying or transmission of confidential information.

9.1.2 A comprehensive data loss prevention (DLP) strategy should be developed to protect confidential and sensitive data, taking into consideration the following specifications:

a. Data at endpoint - Data which resides in notebooks, personal computers, portable storage devices and mobile enterprise devices;

b. Data in motion - Data that traverses a network or transported between sites; and

c. Data at rest - Data in computer storage which includes files stored on servers, databases, backup media and storage platforms.

9.1.3 To achieve adequate security of data at endpoints, FIs should implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres. Confidential customer information stored in all types of endpoint devices should be properly protected with strong encryption.

9.1.4 The use of insecure internet services such as social media sites, cloud-based internet storage sites, and web-based emails to communicate or store confidential information should not be allowed. Measures should be implemented to prevent and detect the use of such services within the organisation.

9.1.5 For the purpose of exchanging confidential information between an FI and its external party, affiliates, partners and regulatory authorities, utmost care must be taken to preserve the confidentiality of the information. Appropriate measures including sending information through encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length for such purposes should be implemented. The encryption key should also be sent via a separate transmission channel to the intended recipients. Alternatively, the FI could choose other secure means to exchange confidential information with its intended recipients.

9.1.6 Backup tapes or disks, including USB drives, of systems which contain sensitive customer information, must be encrypted before they are transported offsite for storage.

9.1.7 Sensitive information stored on IT systems, servers and databases should be encrypted and protected through strong access controls, bearing in mind the principle of “least privilege”.

9.1.8 Measures to prevent the loss of confidential information through disposal of IT systems should be implemented. Various methods in which data could be securely removed from the storage media should be explored and assessed. Security requirements of data residing on the media should be taken into consideration to determine the appropriate media sanitisation method.

9.2 Technology Refresh Management

9.2.1 To facilitate the tracking of IT resources, an up-to-date inventory of software and hardware components used in the production and disaster recovery environments should be maintained.

9.2.2 The IT systems and software should be actively managed so that outdated and unsupported systems which significantly increase an FI’s exposure to security risks are replaced on a timely basis. Particularly, a close attention should be paid to the product’s end-of-support (EOS) date. Vendors will typically cease to provide patches for security vulnerabilities uncovered after the product's EOS date.

9.2.3 A technology refresh plan should be established to replace systems and software in a timely manner. Risk assessment should be conducted for systems approaching EOS dates to assess risks of continued usage. Effective risk mitigation controls should be established accordingly.

9.3 Networks and Security Configuration Management

9.3.1 IT systems and devices should be configured with security settings that are consistent with the level of protection required. Baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices should be established for deployment within the IT environment.

9.3.2 Regular enforcement checks should be conducted to ensure baseline standards are applied uniformly and non-compliances are detected for further investigation. The frequency of enforcement reviews should be commensurate with the risk level of systems.

9.3.3 Anti-virus software should be deployed to servers and workstations. Anti-virus definition files should be regularly updated and automatic anti-virus scanning should be scheduled on servers and workstations on a regular basis.

9.3.4 Network security devices such as firewalls as well as intrusion detection and prevention systems at critical junctures of its IT infrastructure should be installed to protect the network perimeters. Firewalls should also be deployed within internal networks to minimise security exposures originating from third party or overseas systems. In addition, firewall rules should be backed up and reviewed for appropriateness and validity on a regular basis.

9.3.5 FIs deploying Wireless Local Area Networks (WLAN) within the organisation should be aware of risks associated in this environment. Measures, such as secure communication protocols for transmissions between access points and wireless clients, should be implemented to secure the corporate network from unauthorised access.

9.4 Vulnerability Assessment and Penetration Testing

9.4.1 Vulnerability assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system. VAs should be regularly conducted, at least on a quarterly basis, to detect security vulnerabilities in the IT environment.

9.4.2 A combination of automated tools and manual techniques should be deployed for effective VAs. For web-based external facing systems, the scope should include common web vulnerabilities such as SQL injection and cross-site scripting.

9.4.3 A process to remedy issues identified in VAs should be established. Subsequent validation of the remediation should be performed to validate that gaps are addressed appropriately.

9.4.4 Penetration tests with the objective of conducting an in-depth evaluation of the security posture of the system should be carried out by simulating actual attacks on the system. Penetration tests on internet-facing systems should be conducted at least annually.

9.5 Patch Management

9.5.1 A patch management process including instructions on deployment of security patches to the FI's systems and applications should be put in place.

9.5.2 For effective application of security patches, the patch management process should include identification, categorisation and prioritisation of security patches to be released to the production environment. To implement security patches in a timely manner, the implementation timeframe for each category of security patches should be established.

9.5.3 The application of patches, if not carried out appropriately, could potentially impact other peripheral systems. Rigorous testing of security patches should be performed before deploying them into production environment.

9.6 Security Monitoring

9.6.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt identification of unauthorised activities, appropriate security monitoring systems and processes should be established to detect malicious activities stemming from internal staff or external parties.

9.6.2 Network surveillance and security monitoring procedures with the use of network scanners, intrusion detection and prevention systems (IDPS) should be implemented to protect FIs against network intrusion attacks as well as provide alerts to responsible staff when an intrusion occurs.

9.6.3 Security monitoring tools which enable the detection of unauthorised changes to critical IT resources such as databases, system or data files and programs should also be implemented.

9.6.4 Real-time monitoring of security events for critical systems and applications should be instituted to facilitate prompt detection of malicious intent on these systems and applications.

9.6.5 As a form of detection control, security logs of systems, applications and network devices should be regularly reviewed for anomalies.

9.6.6 System logs should be adequately protected and retained to facilitate investigation if need be. Legal and regulatory requirements should be taken into consideration when determining the log retention period.

10 DATA CENTRES PROTECTION AND CONTROLS

10.0.1 As FIs' critical systems, applications, network devices and data are concentrated and maintained in the data centre (DC), it is important that the data centre is resilient and physically secured from internal and external threats.

10.1 Threat and Vulnerability Risk Assessment (TVRA)

10.1.1 The purpose of a Threat and Vulnerability Risk Assessment (TVRA) is to identify security threats to and operational weaknesses in a DC in order to determine the level and type of protection that should be established to safeguard it.

10.1.2 The assessment of threats and vulnerabilities relating to a DC will vary depending on a number of factors, such as geographical location, multi-tenancy and type of tenants occupying the DC. The TVRA assessment should be based on various possible scenarios of threats which include theft, explosives, arson, unauthorised entry, external attacks and insider sabotage.

10.1.3 The scope of the TVRA review should include the perimeter and surrounding environment, building and data centre facility. The review should take into account daily security procedures, critical mechanical and engineering systems, building and structural elements as well as physical, operational and logical access controls.

10.1.4 As part of an FI's mandatory criteria for selecting a DC provider, the FI, which is seeking to procure DC services, should obtain and assess the TVRA report on the DC facility. The FI should verify that TVRA reports are current and that the DC provider is committed to address all material vulnerabilities identified. For an FI that chooses to build its own DC, an assessment of threats and vulnerabilities should be performed at the feasibility study stage.

10.2 Physical Security

10.2.1 Access to DC should be limited to authorised staff and personnel only. Request for access to the DC should be granted on a need to have basis. Personnel working in DC should have his access revoked immediately once his access is no longer required to minimise the risks of internal sabotage.

10.2.2 For non-DC personnel such as vendors, system administrators or engineers who may require temporary access to the DC to perform maintenance or repair work, proper notification and approval should be obtained for such visits. Visitors must be accompanied at all times by an authorised employee while in the DC.

10.2.3 The perimeter of the DC, DC building, facility, and equipment room should be physically secured and monitored. Physical, human and procedural controls such as the use of security guards, card access systems, mantraps and bollards should be employed.

10.2.4 Within the DC, security systems and surveillance tools should be appropriately deployed to monitor and record activities. Physical security should be established to prevent unauthorised access to systems, equipment racks and tapes.

10.3 Data Centre Resiliency

10.3.1 For data centre resiliency, redundancy and fault tolerance should be adequately considered in areas such as electrical power, air conditioning, fire suppression and data communications.

10.3.2 The environment within a DC should be rigorously controlled and regulated. Monitoring of environmental conditions, such as temperature and humidity, within a DC is critical in ensuring uptime and system reliability. Any abnormality detected should be promptly escalated to management and addressed in a timely manner.

10.3.3 Appropriate fire protection and suppression systems should be implemented in the DC to control a full scale fire if it develops. Smoke detectors and hand-held fire extinguishers should also be installed in the DC for early detection and putting out of a developing fire. Passive fire protection elements, such as fire walls around the DC, should also be implemented to restrict the spread of a fire to a portion of the facility.

10.3.4 To minimise downtime from power disruptions, backup power consisting uninterruptible power supplies, battery arrays, and/or diesel generators should be used.

11 ACCESS CONTROL

11.0.1 Three of the most basic internal security principles[10] 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 may include critical systems initialisation and configuration, PIN generation and creation of cryptographic keys and the use of administrative accounts.

b. Segregation of duties principle - Segregation of duties is an essential element of internal controls. Responsibilities and duties for operating systems function, systems design and development, application maintenance programming, access control administration, data security, librarian and backup data file custody should be separated and performed by different groups of personnel. 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.

11.1 User Access Management

11.1.1 User access to IT systems and networks should only be granted on a need-to-use basis and within the period when the access is required. All requests to access IT resources must be duly authorised and approved by the resource owner.

[10] 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.

11.1.2 Personnel from vendors, service providers or consulting firms, who are given authorised access to an FI's critical networks and computer resources, pose similar risks as its internal staff. These external personnel should be subject to close supervision, monitoring and access restrictions similar to those required of internal personnel.

11.1.3 For accountability and identification of unauthorised access, records of user access should be uniquely identified and logged for audit and review purposes.

11.1.4 Regular reviews of user access privileges to verify that privileges are granted appropriately and according to the 'least privileged' principle should be performed. The process may facilitate the identification of dormant and redundant accounts as well as detection of wrongly provisioned access.

11.1.5 Passwords represent the first line of defence, and if not implemented appropriately, they can be the weakest link in the organisation. Thus, strong password controls over users' access to applications and systems should be enforced. Password controls should include a change of password upon first logon, minimum password length and history, password complexity as well as maximum validity period.

11.1.6 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.

11.2 Privileged Access Management

11.2.1 Information 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 should be placed under close scrutiny. Stringent selection criteria and thorough screening should be applied in appointing personnel to critical operations and security functions.

11.2.2 Some common tactics used by insiders to disrupt operations include planting logic bombs, installing stealth scripts and creating system backdoors to gain unauthorised access as well as sniffing and cracking passwords. System administrators[11], IT security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on critical systems they maintain or operate by virtue of their job functions and privileged access.

11.2.3 Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures. The following control and security practices should be adopted:

a. Implement two-factor authentication for privileged users;

b. Institute strong controls over remote access by privileged users;

c. Restrict the number of privileged users;

d. Grant privileged access on a "need-to-have" basis;

e. Maintain audit logging of system activities performed by privileged users;

f. Disallow privileged users from accessing systems logs in which their activities are being captured;

g. Review privileged users' activities on a timely basis;

h. Prohibit sharing of privileged IDs and their access codes;

i. Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and

j. Protect backup data from unauthorised access.

[11] 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.

12 ONLINE FINANCIAL SERVICES

12.0.1 Whilst the internet presents opportunities for FIs to reach new markets and expand its range of products and services, being an open network, it also brings about security risks that are more sophisticated and dynamic than closed networks and proprietary delivery channels. An FI should be cognisant of risks that are brought upon by offering its financial services via the internet platform.

12.0.2 There are varying degrees of risks associated with types of services provided over the internet. Typically, financial services offered via the internet can be classified into information service[12], interactive information exchange service[13] and transactional service[14].

12.0.3 The highest level of risk is associated with transactional service as online transactions are often irrevocable once executed. FIs should clearly identify risks associated with types of internet services being offered in the risk management process. Security controls, system availability and recovery capabilities, which commensurate with the level of risk exposure, should be formulated for all internet operations.

12.1 Online Systems Security

12.1.1 More attacks will be targeted at FIs' internet systems as more financial services are being provided via the internet and more customers transacting on this platform. As a counter-measure, a security strategy should be devised and a suite of measures should be instituted to ensure the confidentiality, integrity and availability of data and systems.

12.1.2 Assurance should be provided that online login access and transactions performed over the internet are adequately protected and authenticated. In addition, customers should be adequately educated on security measures that must be put in place to protect their interests in online environment.

[12] Information service 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.

[13] Interactive information exchange service allows customers to communicate with the FI, make account enquiries and fill in application forms to take up additional services or purchase new products offered.

[14] Transactional service allows customers to execute online transactions such as the transfer of funds, payment of bills and other financial transactions.

12.1.3 It is expected that an FI will properly evaluate security requirements associated with its internet systems and adopt encryption algorithms which are of well-established international standards and subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies. (Refer to Appendix C on Cryptography for details.)

12.1.4 Information processed, stored or transmitted between an FI and its customers should be accurate, reliable and complete. With internet connection to internal networks, financial systems and devices may now be potentially accessed by anyone from anywhere at any time. The FI should implement physical and logical access security to allow only authorised personnel to access its systems. Appropriate processing and transmission controls should also be implemented to protect the integrity of systems and data.

12.1.5 Monitoring or surveillance systems should be implemented to alert FIs of any erratic system activities, transmission errors or unusual online transactions. A follow-up process should be established to verify that these issues or errors are adequately addressed subsequently.

12.1.6 High resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment) should be maintained to meet customers' expectations. Measures to plan and track capacity utilisation as well as guard against online attacks should be established. These online attacks could include denial-of-service attack (DOS attack) or distributed denial-of-service attack (DDOS attack). (Refer to Appendix D for details).

12.1.7 FIs should implement two-factor authentication[15] at login for all types of online financial systems and for authorising transactions. The primary objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in online systems by combating phishing, keylogging, spyware, malware, middleman attacks and other internet-based scams and malevolent exploits targeted at FIs and their customers.

12.1.8 Appropriate measures should also be implemented to minimise exposure to other forms of cyber attacks such as middleman attack which is more

[15] Two factor authentication for system login and transaction authorisation can be based on any two of the factors, i.e. What you know (e.g. PIN), What you have (e.g. OTP token) and Who you are (e.g. Biometrics).

commonly known as a man-in-the-middle attack (MITMA)[16], man-in-the browser attack or man-in-the application attack (refer to Appendix E for details).

12.1.9 As more customers log into FIs' websites to access their accounts and conduct a wide range of financial transactions for personal and business purposes, a suite of measures must be established to protect customers' interests in using online systems. Furthermore, customers should be educated on the risks of using online financial services before they subscribe to such services. Continual education must be available to raise the security awareness of customers to protect their systems and online transactions. (Refer to Appendix F for details on Customer Protection and Education).

12.2 Mobile Online Services and Payments Security

12.2.1 Mobile Online Services refers to the provision of financial services via mobile devices such as mobile phones or tablets. Customers could choose to access these financial services via web browsers on mobile phones or an FI's self-developed applications on mobile platforms such as Apple's iOS, Google's Android and Microsoft's Windows operating systems.

12.2.2 Mobile payment refers to the use of mobile devices to make payments to merchants for purchases. These payments could be made using various technologies such as near field communication (NFC).

12.2.3 Mobile online services and payment are extensions of the online financial services and payments services which are offered by FIs and accessible from the internet via computers or laptops. Security measures which are similar to those of online financial and payment systems should also be implemented on the mobile online services and payment systems. A risk assessment should be conducted to identify possible fraud scenarios and appropriate measures should be established to counteract payment card fraud via mobile devices.

12.2.4 FIs may require customers to download its mobile online services and payment applications directly from third party repositories (e.g. Apple store, Google Play and Windows Market Place) on to mobile devices. Customers must be able to verify the integrity and authenticity of the application prior to its

[16] 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.

download. FIs should also be able to check the authenticity and integrity of the software being used by the customers.

12.2.5 As mobile devices are susceptible to theft and loss, there must be adequate protection of sensitive data used for mobile online services and payments. Sensitive data should be encrypted to ensure the confidentiality and integrity of these data in storage, transmission and during processing.

12.2.6 Customers should be educated on security measures to protect their own mobile devices from theft and loss as well as viruses and other errant software which cause malicious damage and harmful consequences.

13 PAYMENT CARD SECURITY (ATM, CREDIT AND DEBIT CARDS)

13.0.1 Payment cards[17] allow cardholders the flexibility to make purchases wherever they are. Cardholders could choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase their items over the internet, through mail-order or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines (ATMs) or merchants.

13.0.2 Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including payment kiosks[18] and EFTPOS terminals.

13.0.3 Besides counterfeit cards, fraudulent activities associated with payment cards include lost/stolen cards, card-not-received[19] (CNR) and card-not-present[20] (CNP) transactions.

13.1 Counteract Payment Card Fraud

13.1.1 FIs which provide payment card services should implement adequate safeguards to protect sensitive payment card data. Sensitive payment card data should be encrypted to ensure the confidentiality and integrity of these data in storage, transmission and during processing.

13.1.2 Secure chips should be deployed to store sensitive payment card data. Strong card authentication methods such as dynamic data authentication (DDA) or combined data authentication (CDA) methods for online and offline card transactions should be implemented. As magnetic stripe cards are vulnerable to card skimming attacks, magnetic stripes should not be used as a means to store sensitive data for payment cards.

[17] For the purpose of this document, payment cards refer to ATM, credit, charge and debit cards.

[18] For the purpose of this document, kiosks refer to ATMs and merchant provided 24-hour payment booths such as self-service automated machines (SAM) and AXS machines.

[19] Card-Not-Received (CNR) fraud refers to fraud cases where cardholders do not receive cards dispatched by the issuing banks and subsequently, these cards are used to make fraudulent transactions.

[20] Card-Not-Present (CNP) fraud involves the use of stolen or compromised card details to make purchases over the internet, phone or mail order catalogues. There is also a rising trend in CNP transactions in the form of online payment transactions.

13.1.3 FIs should only allow online transaction authorisation. Authentication of customers' sensitive static information, such as personal identification number (PIN) or passwords, should be performed by the card issuer and not by third party payment processing service providers. Regular security reviews of the infrastructure and processes at its service providers should be performed.

13.1.4 Security controls should be implemented at payment card systems and networks. These systems should be enhanced with the most recent and stable security version.

13.1.5 New payment cards sent to customers via post should only be activated upon obtaining the customer's instruction. A dynamic one-time-password should also be implemented for CNP transactions via internet to reduce fraud risk associated with CNP.

13.1.6 To enhance card payment security, cardholders should be notified promptly via transaction alerts on withdrawals / charges exceeding customer-defined thresholds made on their payment cards. The transaction alert should include information such as source and amount of the transaction to assist customers in identifying a genuine transaction.

13.1.7 Fraud detection systems with behavioural scoring and correlation capabilities should be implemented to identify and curb fraudulent activities. Risk management parameters should be calibrated according to risks posed by cardholders, nature of transactions or other risk factors to enhance fraud detection capabilities.

13.1.8 Follow-up actions for transactions exhibiting behaviour which deviates significantly from a cardholder's usual card usage patterns should be instituted. These transactions should be investigated into and the cardholder's authorisation obtained prior to completing the transaction.

13.2 ATMs and Payment Kiosks Security

13.2.1 The presence of ATMs and payment kiosks (e.g. SAM and AXS machines) has provided cardholders with the convenience of withdrawing cash as well as making payments to billing organisations. However, there are cases where fraudsters exploit weaknesses pertaining to the ATM systems that resulted in their success in stealing cardholders' payment card details and PINs.

13.2.2 To secure consumer confidence in using these systems, the following measures should be considered to counteract fraudsters' attacks at the ATMs or payment booths:

a. Install anti-skimming solutions on these machines or booths to detect the presence of foreign devices placed over or near a card entry slot;

b. Install detection mechanisms and send alerts to appropriate personnel for follow-up response and action;

c. Implement tamper-resistant keypads to ensure that no one can identify which buttons are being pressed by customers;

d. Implement appropriate measures to prevent shoulder surfing of customers' PINs; and

e. Conduct video surveillance of activities at these machines or booths; and maintain the quality of CCTV footage.

13.2.3 FIs should also verify that adequate physical security measures at payment booths are provided by third party, which are used to accept and process the FIs' payment cards.

14 IT AUDIT

14.0.1 As technology risks evolve with the growing complexity of the IT environment, there is an increasing need for FIs to develop effective internal control systems to manage technology risks.

14.0.2 IT audit provides the board and senior management with an independent and objective assessment of the effectiveness of controls that are applied within the IT environment in managing technology risks.

14.0.3 The IT audit organisational structure and reporting lines should be established in a way that independence and objectivity of the IT audit function are preserved. In addition, the IT audit personnel must not participate in any activities that may compromise his or her independence.

14.1 Audit Planning

14.1.1 The scope of IT audit should be wide-ranging and include the critical IT operations.

14.1.2 A well-defined audit universe encompassing auditable entities pertaining to IT operations should also be established. These auditable entities should be discrete segments that allow IT auditors to perform an effective risk assessment of the IT operation, administration, security and infrastructure in order to formulate their audit plan.

14.1.3 With changes in the IT operating environment, emerging threats as well as new business areas, IT auditors should update the audit universe periodically to reflect these changes.

14.1.4 An IT audit plan, which comprises auditable IT areas for the coming year, should be established and approved by Audit Committee. In addition, the Audit Committee should be kept apprised of changes to the audit plan such as change in IT audit scope and schedule.

14.1.5 An audit cycle that identifies the frequency of IT audits should be established. Auditors should determine the frequency based on results of risk assessments. Audits of high-risk IT areas should be performed on an annual basis.

14.2 Remediation Tracking

14.2.1 A follow-up process to track and monitor IT audit issues should be established. Examination findings issued by MAS should be verified and validated by internal auditors prior to closure.

14.2.2 An escalation process should be established to notify relevant management at an FI of overdue IT audit issues or unsatisfactory responses to the issues. In addition, recurring IT audit issues should be escalated to the senior management, audit committee and the board.

APPENDIX A: SYSTEMS SECURITY TESTING AND SOURCE CODE REVIEW

A.1 Overview

A.1.1 Rigorous testing on systems must be conducted to verify the security, reliability and availability of its systems under normal or extreme conditions. However, security testing is ineffective in identifying or detecting security threats and weaknesses such as malicious codes, trojans, backdoors, logic bombs and other malware. Thus, source code review should be included into its system development life cycle (SDLC) to identify and detect such threats and weaknesses in its systems.

A.1.2 While testing methodologies may differ for various applications, the following areas should be included into both the testing and source code review process:

a. Identify Information Leakage

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.

Tests should also be carried out to detect network system verbosity and promiscuity.

b. Assess Resiliency Against Input Manipulation

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.

All input validation routines should be reviewed to assess their effectiveness against known vulnerabilities by appropriate testing.

c. Identify insecure programming practices

The source code review 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.

Appropriate tests should be carried out to ascertain that security weaknesses due to insecure programming practices are not present in the systems.

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.

Authentication testing should ensure that security requirements (such as credential expiry, revocation and reuse) are implemented correctly and the protection of security functions and cryptographic keys is robust.

Session management should be tested to ensure that :

i. Sensitive information that is passed in the cookies is encrypted.

ii. The session identifier is random and unique.

iii. The session expires after a pre-defined length of time.

e. Cryptography

Cryptography is employed to protect sensitive data. The strength of cryptography depends not only on the algorithm and key size, but also on its implementation.

Cryptographic implementation should be evaluated and 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.

In addition, 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). Refer to Appendix C for more details.

f. 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.

In addition, stringent exception/error handling that facilitates fail-safe processing under various error, exception or erratic conditions should be implemented. Stress testing outside the stated limits of the systems should be conducted to verify that the application still works correctly albeit with degraded service levels. Leakage of sensitive information should not be an outcome of a system failure.

A.1.3 An FI should also include the following areas into its security testing:

a. Business Logic

Business logic must be adequately tested to avoid mistakes made in implementing business logic that lead to security holes whereby a user may perform an unauthorised function.

b. Authorisation

After a user has been authenticated and gains access into the system, 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 performed to verify that the security access matrix works correctly in various permutations.

c. Logging

Logging is implemented to avoid security defects as well as facilitate follow-up investigation and troubleshooting when a system incident occurs. The following requirements and specifications should be built into the tests:

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.

APPENDIX B: STORAGE SYSTEM RESILIENCY

B.1 Overview

B.1.1 Storage systems are key IT infrastructure components that house critical information assets. The resiliency and availability of these storage systems are crucial to the continuous operation of critical applications and online systems used by FIs.

B.2 Reliability and Resiliency

B.2.1 The architecture and connectivity of storage systems used by critical applications should be regularly reviewed for single points of failure and fragility in functional design and specifications, as well as technical support, whether performed in-house or by vendors. The resiliency of storage systems for both centralised and distributed systems should also be considered.

B.2.2 Where storage area networks (SAN) are deployed, redundancy should be incorporated in all SAN components. Multiple links and switches should be installed for all I/O operations between hosts, adapters, storage processors and storage arrays. Hosts, switches, storage processors and storage arrays should also be properly configured for high availability.

B.2.3 To guard against disk failures in storage arrays, mirrored or parity redundant array of independent disks (RAID) protection should be implemented. Hot spares should also be allocated and configured to reduce the impact of subsequent failures in storage arrays.

B.2.4 To improve the reliability and fault-tolerant capability of storage systems, an FI should establish a sound patch management process to update its storage systems with the latest stable and proven microcode release on a timely basis. The deployment of configuration changes and upgrades to storage systems should be governed by a rigorous change management process.

B.2.5 An in-house alert and monitoring capability should be established for early detection of warnings and outages in its storage systems, as well as data replication mechanisms. The implementation of vendor call-home capability to perform advanced diagnostics and remediation should also be considered. To minimise the risk of multiple failures and human errors, an FI should maintain oversight of diagnostics and remediation activities, whether performed in-house or by vendors.

B.3 Recoverability

B.3.1 In the event of a major site outage, the architecture of the storage system should have the capability to switch over from the primary production site to an alternate site to meet required recovery time objectives (RTOs) and recovery point objectives (RPOs). The recoverability and consistency of data at the alternate site should be regularly tested.

B.3.2 To improve the recoverability of critical services due to component failures, an FI should consider high availability architecture of the storage system at the primary site and preferably also at the alternate site. Such redundancies would provide the FI with more recovery options to manage component failures without resorting to a full disaster recovery invocation. Failover and fallback capabilities should also be regularly tested.

B.3.3 While data replication technology provides high availability, both primary and replicated data sets could be affected by accidental or malicious logical data corruption. Hence, adequate point-in-time copies / snapshots of data should be available for restoration to known consistent states.

APPENDIX C: CRYPTOGRAPHY

C.1 Principles of Cryptography

C.1.1 The primary application of cryptography is to protect the integrity and privacy of sensitive data. Cryptography is also commonly used in FIs to protect sensitive customer information such as PINs relating to critical applications (e.g. ATM, payment cards and online financial systems).

C.1.2 All encryption algorithm used in a cryptographic solution must depend only on the secrecy of the key and not on the secrecy of the algorithm. As such, the most important aspect of data encryption is the protection and secrecy of cryptographic keys used, whether they are master keys, key encrypting keys or data encrypting keys.

C.2 Cryptographic Algorithm and Protocol

C.2.1 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.

C.2.2 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.

C.2.3 Random Number Generators are used in many algorithms and schemes as a construct component. The security of many cryptographic algorithms depends upon the unpredictable quality of a random seed. There must be sufficient size and randomness of the seed number to preclude the possibility of optimized brute force attack.

C.3 Cryptographic Key Management

C.3.1 Cryptographic key management policy and procedure covering generation, distribution, installation, renewal, revocation and expiry should be established.

C.3.2 Cryptographic keys should be securely and properly generated. All materials used in the generation process should be destroyed after usage. 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 stringent conditions.

C.3.3 Unencrypted symmetric keys shall be entered into hardware security module only in the form of at least two components using the principles of dual control and split knowledge.

C.3.4 To minimise the impact when keys are compromised, cryptographic keys should only be used for a single purpose. Key types shall be identified by the usage and each key type shall be protected by a different key encryption key.

C.3.5 The effective timeframe that a cryptographic key could be used in a given cryptographic solution is called the cryptoperiod. FIs should thoroughly consider and decide the appropriate cryptoperiod for each cryptographic key. The sensitivity of data and operational criticality should determine the frequency of key changes.

C.3.6 Hardware security modules and keying materials should be physically and logically protected.

C.3.7 When cryptographic keys are being used or transmitted, these keys must not be exposed during usage and transmission.

C.3.8 When cryptographic keys have expired, a secure key destruction method should be used to ensure keys could not be recovered by any parties.

C.3.9 In the event of changing a cryptographic key, the new key should be independently generated from the previous key.

C.3.10 Backup copies of important cryptographic keys should be securely kept. These backup copies should be subjected to the same level of security control as the original key. Backup keys should be securely stored and separated from the storage of the original key. The storage duration should be similar to the cryptoperiod of the original key. During the destruction of the original key, the backup key should also be destroyed at the same time.

C.3.11 FIs may need to archive their cryptographic keys for verification of the integrity of past transactions. The key used to encrypt the original key must not be used to encrypt archived keys. The storage duration of archived keys should be similar to the cryptoperiod of the original key.

C.3.12 If a key is compromised, the key, its variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key shall be destroyed and replaced. Compromised keys should be immediately revoked and all parties concerned are informed.

C.3.13 A process for the replacement of compromised keys without major impact to the existing operations should be established.

APPENDIX D: DDOS PROTECTION

D.1 Overview

D.1.1 Although Distributed Denial of Service (DDoS) attacks have always posed a formidable threat to internet systems, the proliferation of botnets 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.

D.1.2 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.

D.1.3 Notwithstanding that most FIs have instituted effective safeguards to protect its 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.

D.2 Detecting and Responding to DDoS Attacks

D.2.1 FIs providing online financial services should be responsive to unusual 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.

D.2.2 As part of the defence strategy, FIs 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 and trading systems could flow through.

D.2.3 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.

D.3 Selection of Internet Service Providers (ISPs)

D.3.1 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.

D.3.2 Given that a collaborative approach should be adopted by FIs and its ISPs, it is important that FIs incorporate DDoS attack considerations in its ISP selection process which should include determining:

a. whether an ISP offers DDoS protection or clean pipe services to assist in detecting and deflecting malicious traffic;

b. the ability of the ISP to scale up network bandwidth on demand;

c. the adequacy of an ISP's incident response plan; and

d. the ISP's capability and readiness in responding quickly to an attack.

D.4 Incident Response Planning

D.4.1 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.

D.4.2 FIs should be familiar with the ISPs' incident response plans and assimilate them into its incident response framework. To foster better co-ordination, a communication protocol should be established between an FI and its ISPs and periodic joint incident response exercises conducted.

APPENDIX E: SECURITY MEASURES FOR ONLINE SYSTEMS

E.1 Overview

E.1.1 A man-in-the-middle attack refers to a scenario where 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.

E.1.2 There are many possible attack points for MITMA. They could be at customer computers, internal networks, information service providers, web servers or anywhere in the internet along the path between the user and an FI's server.

E.2 Security Measures

E.2.1 As part of the two-factor authentication infrastructure, the following control and security measures should be implemented to minimise exposure to man-in-the middle attacks:

E.2.2 Transaction signing for high-risk as well as high-value transactions

a. Digital signatures and key-based message authentication codes (KMAC) are used for transaction-signing of high-risk or high-value transactions for the detection of unauthorised modification or injection of transaction data in a MITMA.

b. High-risk transactions would include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details and revision of funds transfer limits.

c. 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. For example, for payment of funds, the token should at least explicitly show the hash value to be signed together with the payee account number and the payment amount from which the hash value is derived.

d. Different crypto keys should be used for generating OTPs and for signing transactions.

E.2.3 OTP time window

a. FIs may choose to implement challenge-based or time-based one-time-passwords (OTPs) for its online systems. These provide strong security because their period of validity is controlled entirely by FIs and does not depend on the behaviour of the user.

b. Due to time synchronisation problems, the use of time-based OTPs requires a time window at the server-side. FIs 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 risks of OTP misuse.

E.2.4 Second channel notification / confirmation

a. FIs should notify their customers, through a second channel, of all high-risks transactions as well as payment or fund transfer transactions above a specified value determined by customer.

b. Meaningful information such as type of transaction and payment amounts should be provided promptly in the notification after the transaction.

c. The notification should be sent to the customer on a separate device other than the device used to perform the transaction.

E.2.5 End-to-end encryption security at application layer

a. End-to-end encryption security should be implemented at the application layer for its internet systems so that customer PINs and passwords are not exposed at any point of the systems.

E.2.6 Session time-out

a. 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 session alive indefinitely.

E.2.7 SSL server certificate warning

a. Customers using the internet application 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 FI and a warning is given to this effect. Customers should inform the FI immediately after logging

APPENDIX F: CUSTOMER PROTECTION AND EDUCATION

F.1 Overview

F.1.1 Direct attacks on online financial systems have caused customer PINs to become increasingly vulnerable. Through targeted attacks, customer PINs are under constant threats from various types of systems vulnerabilities, security flaws, exploits and scams. An FI has the responsibility to ensure that customers' accounts and data are protected upon using online financial services as well as raising their security awareness to prevent falling into traps set by scammers.

F.2 Customer Protection

F.2.1 FIs should not distribute software to its customers via the internet or through a web-based system unless they can provide adequate security and safeguards for the customers. This is to avoid the situations whereby customers are deceived by hackers into downloading trojans, backdoors, viruses and other errant software which cause malicious damage and harmful consequences to their personal customers. Customers should be provided with mechanisms to verify the origin and integrity of the downloaded software and authenticate the FI's digital signature incorporated in the software using a digital certificate provided by the FI. In return, the FI should be able to check the authenticity and integrity of the software being used by customers.

F.2.2 To ensure that customers are properly identified and authenticated in online systems, FIs should establish the following measures to protect login credentials of customers:

a. Implement dual control and segregation of duties in the generation of passwords, printing of password mailers and activation of online accounts;

b. Print password mailers in a secure location where physical access is restricted and monitored;

c. Destroy all mailer spoilages immediately and generate a new password for each reprint;

d. Destroy all stationery which may contain any password imprint during mailer printing;

e. Strengthen password dissemination process to ensure that clear-text passwords are not being exposed or compromised;

f. Ensure that passwords are not processed, transmitted or stored in cleartext;

g. Require customers and system users to change issued passwords immediately upon first login; and

h. Mail out hardware token that is assigned to a particular customer account.

F.2.3 Clear information should be provided to customers about the risks and benefits of using online financial services before they subscribe to such services. Customers should be informed clearly and precisely on the respective rights, obligations and responsibilities of the customers and the FI on all matters relating to online transactions, and in particular, any problems that may arise from processing errors and security breaches. Information should not be represented in prolix legalese or technical terminology as it would cause legibility and comprehension difficulties for customers.

F.2.4 The terms and conditions applying to online financial services should be readily available to customers within the internet 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.

F.2.5 Other forms of disclosures that should be posted on the FI's website include :

a. Customer privacy and security policy.

b. Customer dispute handling, reporting and resolution procedures, including the expected timing for the FI's response. The website should contain an explanation on the process 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 FI or its customers if security breaches occur and customer online accounts might have been fraudulently accessed and unauthorised transactions made. Information provided should be useful and relevant for the customers in making informed decisions.

c. 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.

F.2.6 An FI should automatically terminate an online session 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 session alive indefinitely. In addition, 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.

F.3 Customer Education

F.3.1 Customers should be educated on the security and reliability of their interaction with FIs. Customer's confidence in the safety and soundness of the FI'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 online accounts and transaction services. In addition, it is 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 transactions.

F.3.2 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, FIs 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.

F.3.3 To raise security awareness, FIs 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:

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

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

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

d. PIN must be memorised and not be recorded anywhere.

e. PIN should be changed regularly.

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

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

h. Customer should check the authenticity of the FI's website by comparing the URL and the FI's name in its digital certificate or by observing the indicators provided by an extended validation certificate. If the certificate does not belong to the FI and a warning is given to this effect, customer should inform the FI immediately after logging off.

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

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

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

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

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

n. Customer should inform the FI immediately on the loss of his mobile phones or change in his mobile numbers.

F.3.4 Customers should be advised to adopt the following security precautions and practices:

a. Install anti-virus, anti-spyware and firewall software in their personal computers and mobile devices.

b. Update operating systems, anti-virus and firewall products with security patches or newer versions on a regular basis.

c. Remove file and printer sharing in computers, especially when they are connected to internet.

d. Make regular backup of critical data.

e. Consider the use of encryption technology to protect highly sensitive data.

f. Log off the online session.

g. Do not install software or run programs of unknown origin.

h. Delete junk or chain emails.

i. Do not open email attachments from strangers.

j. Do not disclose personal, financial or credit card information to little-known or suspect websites.

k. Do not use a computer or a device which cannot be trusted.

l. Do not use public or internet café computers to access online services or perform financial transactions.

F.3.5 In view of the widespread of payment cards such as ATM, credit and debit cards used by customers, customers should be educated on the features of these cards as well as their associated risks. In addition, adequate information and instruction should be provided to ensure that customers understand the measures of how to ensure the security of their cards and the steps required in reporting card loss or fraud cases.

F.3.6 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.