



Monetary Authority of Singapore

TECHNOLOGY RISK
MANAGEMENT GUIDELINES
FOR FINANCIAL INSTITUTIONS

**Draft Version 1.1
as at 28 February 2003**

Consultation Draft for Comments

Issued: 11 November 2002
Due date: 11 December 2002

Please forward your comments to Mr Tony Chew, Director, Technology Risk Supervision
Monetary Authority of Singapore, 10 Shenton Way MAS Building, Singapore 079117
Telephone: 62299109 Fax: 62299659 Email: tonychew@mas.gov.sg

TABLE OF CONTENTS

1.0	INTRODUCTION	1
2.0	TECHNOLOGY RISK DIMENSIONS	2
3.0	TECHNOLOGY RISK MANAGEMENT	4
4.0	ISSUES IN INFORMATION SECURITY	6
5.0	IDENTIFICATION AND AUTHENTICATION	8
6.0	AUTHORISATION AND ACCOUNTABILITY	10
7.0	TECHNOLOGY RISK GUIDELINES	11
7.1	DELINEATE RESPONSIBILITY FOR SAFETY AND SOUNDNESS	11
7.2	ESTABLISH RESPONSIBILITY FOR MANAGING TECHNOLOGY RISKS.....	11
7.3	NURTURE A RISK AWARENESS CULTURE	12
7.4	RECTIFY THE WEAKEST SECURITY LINK	13
7.5	CONDUCT VULNERABILITY AND SECURITY ASSESSMENT	13
7.6	INVEST IN SYSTEM AVAILABILITY AND INTEGRITY.....	14
7.7	PREPARE FOR CONTINGENCIES AND DISRUPTIONS	14
7.8	EDUCATE CUSTOMERS ON SECURITY PRECAUTIONS	15
7.9	MANAGE OUTSOURCING RISKS	17
	<i>APPENDIX A – TECHNOLOGY RISK DIMENSIONS</i>	<i>19</i>
	<i>APPENDIX B – INTERNAL CONTROL PRINCIPLES</i>	<i>20</i>
	<i>APPENDIX C – SECURITY PRACTICES FOR FINANCIAL INSTITUTIONS</i>	<i>21</i>
	<i>APPENDIX D – SECURITY PRECAUTIONS FOR CUSTOMERS</i>	<i>23</i>
	<i>APPLICABILITY OF THESE GUIDELINES</i>	<i>25</i>

1.0 INTRODUCTION

1.0.1 Technology does not slow down for anyone. Its pace of change will most likely continue to accelerate in the coming years. The scope and reach of computer systems in the financial industry have risen exponentially, especially those providing web-based services. Many of these computers may not have been properly configured to block hacking intrusions and malware infiltration as they are set at the default level to facilitate easy installation and accessibility. On account of these developments, technology risks¹ and information security issues have become progressively more complex and pressing in recent years due to the constant infusion of new technologies which permeates the financial industry.

1.0.2 Information security has never been more significant than in today's world of heightened security risks and threats. This security focus is just as important as the new technologies being deployed in the financial industry. Intrusions and other forms of attacks on computer systems will not only persist but they will continue to proliferate in frequency and propagate in magnitude. The nature of hacking attacks on computer systems has become increasingly sophisticated and malevolent. While most security spending in recent years is aimed at fortifying perimeter defence to keep external attackers at bay, there is a growing realisation that an attack from within could be far more ominous and perilous. Furthermore, acts of terrorism and cyber warfare are additional risks which financial institutions need to factor into their contingency planning.

1.0.3 Financial institutions should adopt a defence-in-depth approach towards information security. This means having security strategies of prevention and detection so that they know when they are under attack and have the necessary response to counter any incursion. And equally important, they should know where, in their computer systems, intruders can go once they get through their defence and what they might do once they get there.

1.0.4 A resilient technology risk management system requires the establishment of a security posture which protects the information assets of the organisation² and maintains a proactive stance to deal with adverse events or incidents which may strike unexpectedly. A rapid recovery capability under stress conditions of this nature is crucial. The continuing ability of key personnel who can keep the business going and the support operations running is indispensable

¹ Technology risks are defined as any potential adverse outcome, damage, disruption, violation, failure or loss arising from the use of or reliance on computer hardware, software, systems, applications and networks. These risks are usually related to systems flaws, processing errors, software defects, operating mistakes, procedural faults, systems failures, capacity inadequacies, hardware breakdowns, network vulnerabilities, control weaknesses, security deficiencies, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities.

² Organisations and institutions are used interchangeably to mean financial institutions.

in enabling the organisation to overcome operational disruption and adversity. It is senior management's responsibility to ensure the organisation has the capacity and preparedness to deal with such eventualities.

1.0.5 A security posture is not just about installing the latest security devices and deploying the most advanced security technologies. It should incorporate people, policies and processes. There should be a structured, cohesive program to educate management, staff, customers and users³.

1.0.6 The purpose of this document is to make financial institutions aware of the myriad dimensions of technology risks, and the actions they should take to improve information technology security and protect their information assets. A robust technology risk management framework should include the following requirements:

- Compile an inventory of the information assets of the organisation.
- Determine and prioritise those assets which need protection.
- Ascertain what vulnerabilities and threats affect those assets.
- Assess the damage that would be caused to the organisation if the vulnerabilities were successfully exploited by those threats.
- Take appropriate steps to address the vulnerabilities and protect the assets against external and internal threats⁴.
- Implement risk management processes and security measures to safeguard their confidentiality, integrity and availability.

2.0 TECHNOLOGY RISK DIMENSIONS

2.0.1 As the internet is now being utilized for just about every type of financial transaction, it is imperative that the security risks of doing business on the internet be properly understood. It helps to have a good knowledge of the topography of this ubiquitous network infrastructure and the security that is required to protect transactions in transit as well as at various processing nodes and transfer points. The internet has become almost an integral part of most online networking systems.

³ Users refer generally to employees, counterparties, customers, vendors, contractors or anyone permitted to access the institution's systems.

⁴ According to some research surveys, a large percentage of attacks on computer systems are perpetrated by or involved the complicity of insiders such as computer operators, programmers, administrators and other technical staff who have access codes and other sensitive information.

2.0.2 Intrusion detection studies and research honeypot projects have gathered empirical data which showed that the life expectancy of default installations in being attacked was numbered in days. Web servers with default installation settings had been hacked and breached within a couple of days of going live, in some cases within 3 days⁵. On the internet, hacking is omnipresent. It is also persistent. No one is immune.

2.0.3 In the internet cyberspace all computers are equidistant from each other. An attack can be made from a computer anywhere in the world against another computer in another part of the world. Distance and borders are no barriers to cyberspace attacks which are unleashed anonymously, maliciously and indiscriminately.

2.0.4 The growing complexity of internet technologies has continually spawned new risks, vulnerabilities and threats. Complexity and constant changes in systems pose formidable security challenges. The random connectivity and accessibility of networked systems and hosts on the internet creates security exposures which are unprecedented and which are hitherto unknown in proprietary or closed-loop networks. The explosive growth of internet users, together with their inherent anonymity and accessibility to hacking tools, tends to produce a predictable demographic outcome of people who are tempted, hired or lured into committing illegal, nefarious and malevolent acts which they would not otherwise do if they believe they would be tracked down and apprehended.

2.0.5 While security threats are universal to business organisations which share similar vulnerabilities and risks, the consequential damage to a financial institution is more likely to be much greater. This is because of the nature of the business of a financial institution and the scope of its operations. Loss of reputation, customer mistrust, operational impairment, legal implications and regulatory consequences are serious and troubling issues for an institution which has been hacked and its systems compromised.

2.0.6 Security can be regarded as a necessary and prudent cost of doing business safely and soundly. The volume and velocity of online financial transactions have grown tremendously in recent years. Some organisations have rushed into launching online internet systems without due regard for security controls. They might have intended to add security “later”. This does not always occur. Security, when bolted on later, is probably more costly and less effective.

2.0.7 Hacking and malevolent software have increased dramatically in the past few years. They will continue to proliferate and threaten computer systems. Most of the computer technology in use today is not protected by thick walls,

⁵ MAS Specialist Risk Supervision Department operates a security simulation laboratory which has a honeypot website. Within 3 days of going live, the honeypot attracted many hackers from several countries. Their hacking attacks followed a prototypical model which included preliminary probing, vulnerability scanning, forcing entry to install rootkits and scrubbing their footprints.

steel doors, motion sensors, pressure detectors, audio-video devices and armed guards as in the mainframe era. The risk of computer damage, system crash and data loss is not a new concept. Organisations maintain backup data and backup site for disaster recovery purposes.

2.0.8 While protecting computer system facility and its hardware is extremely important, the computer data is far more important than the computer hardware. Computer data can be remotely accessed, altered, deleted, manipulated or inserted without any manifestations of a physical attack or forced entry into a computer centre. Anyone with a web browser and an internet connection may be able to access an organisation's system connected to the internet from anywhere at anytime. Information security is a complex, fast-moving, high-tech field which is almost an industry unto itself, distinct from other computer disciplines.

2.0.9 Financial institutions are targeted by hackers more often and more intensively than other organisations. Financial fraud will be attempted whenever criminals, hackers or thieves see exploitable opportunities. Systems with little or weak security parade such opportunities. It may take only one security incident to cost an organisation substantially more than what it would cost to have good security in the first place.

2.0.10 As a result of recent security events and hacking incidents, institution boards and senior management are becoming more knowledgeable about the density and magnitude of technology risk dimensions⁶ and information security issues. Security exposures which threaten asset safety and share values usually attract the greatest of attention. In many cases, board and management attention is mainly driven by the need to comply with legal and regulatory requirements relating to due diligence and fiduciary duties. They have a fiduciary duty to protect the organisation from serious cybercrime and security risks which may have a catastrophic impact on the organisation's reputation, assets and viability. Technology risks are normally dealt with through a framework of establishing security policies and implementing security measures, including compliance monitoring of security standards approved by the board and senior management.

3.0 TECHNOLOGY RISK MANAGEMENT

3.0.1 Risk management is a familiar concept to the board and senior management of all financial institutions. If there are technology risks serious enough to threaten the well-being and success of the organisation, the board and senior management have a clear responsibility to establish a risk management framework to identify these risks and take adequate measures to address them. The board and senior management should review and approve the organisation's technology risk management policies and information security plans.

⁶ Technology risk dimensions relating to the web and the internet are discussed in Appendix A.

3.0.2 The concept of technology risks and the techniques of technology risk management require a realignment in mindset to understand the paradigm shifts in the way computer systems is being developed and deployed, and how new technologies are impacting the institution's business operations and delivery channels. The computer systems, networks and databases of financial institutions have also become an integral part of the nation's critical financial infrastructure which is increasingly linked to the internet.

3.0.3 Risk management in this new technology-driven environment is no longer a task that is merely carried out once a year. In today's paradigm, risk management has to be regarded as an oversight process undertaken by senior management on a continuous basis. This process involves risk identification, assessment, control and mitigation. The scope of risk management should embrace a broader horizon which incorporates risk anticipation and preclusion. To evaluate risks, it is necessary to make an assessment of vulnerabilities, threats, exposures and the cost of required security measures.

3.0.4 Information security involves a combination of corporate governance, business management and technical issues. Security policies reflect senior management's decisions on what information assets to safeguard, how they should be protected and the responsibilities which accompany various security functions. A policy-driven security program⁷ should include the following actions:

- Evaluate the vulnerabilities, threats and exposures⁸ relating to information assets.
- Determine what control and security measures are required to protect information assets.
- Install firewalls, anti-virus software and intrusion detection systems.
- Deploy strong cryptographic protection of sensitive data.
- Maintain network surveillance and security monitoring.
- Conduct vulnerability assessment and penetration testing.
- Establish a fast incident response and rapid recovery capability.

⁷ Appendix C contains a list of recommended security practices.

⁸ Vulnerabilities are system characteristics or weaknesses which can be exploited to cause loss or harm to an organisation. Threats to computer systems are people, events or conditions which have the potential to cause loss or harm. Exposures are different forms of potential loss or harm which an organisation may suffer due to security weaknesses in its computer systems.

3.0.5 Risk can be regarded as the antithesis of security and safety. The primary aim of risk management is neither total risk avoidance nor elimination but one of risk control and reduction. An effective risk mitigation approach means that a sound knowledge of the level and composition of risks – vulnerabilities, threats, consequences and countermeasures - is necessary in order to prioritise and focus resources on what the key risks are. The rapidity and frequency of systems and operational changes require an ongoing process of assessing new and existing risks and developing a proactive method of dealing with them. In today's fast-paced changing environment, there may be insufficient time to construct a risk mitigation plan between the time the first indication of a security incident is known and the time the consequences take effect. Advance planning and a fast incident response capability are necessary for such eventualities.

3.0.6 The use of technology has its risks. The most prolific of these risks are identity theft, impersonation, unauthorised access, fraud, forgery, hacking, denial of service attacks, sabotage, systems manipulation and systems failure. A good systems control and security program should include the following requirements:

- Implementation of sound security practices.
- Implementation of systems development controls and testing.
- Compliance with legal and regulatory requirements.
- Protection of business reputation.

3.0.7 Conducting business on networked systems, especially on the internet, provides a level of flexibility, convenience and accessibility to customers, suppliers and internal users which few other systems or delivery channels could match. But the additional and heightened risks attached to such network effects are not trivial. Most financial institutions recognise that they are prime targets of attack in the cyber world, just as they are the most attractive targets of robbery and embezzlement attempts in the physical world. They have to take appropriate steps to prevent and detect such attacks by focusing on the vulnerabilities and threats to their systems and the environment they operate in. There are many different ways of defining and evaluating risks. Each organisation has to find and use a methodology which suits its risk management approach and risk tolerance.

4.0 ISSUES IN INFORMATION SECURITY

4.0.1 As technology becomes more complex, the need for security is even greater. In cyberspace, an attack on a computer system can be made by anyone at anytime from anywhere. An attacker with little skill or technical knowledge could obtain open source exploit tools to launch an attack. An elite hacker or professional criminal could create his own special exploits to break into systems.

4.0.2 Every financial institution should have a security policy for its computer systems and networks. Financial institutions need to be mindful of the craftiness and sophistication of potential attacks that could be unleashed by hackers and criminals. Firewalls and intrusion detection tools should be used to protect web servers, applications, databases, hosts and networks by uncovering and blocking malicious actions or intrusions.

4.0.3 Most attacks on financial systems are premeditated and planned. From an institution's standpoint, it is difficult to anticipate or pre-empt what are seemingly random or sudden attacks. Yet, this is exactly what incident response planning should expect. When an attack is underway, it is rather too late to start planning what to do. The incident response plan should provide guidance on how to react to a cyber attack and what containment and remedial actions to take to minimise the potential damage to the organisation.

4.0.4 Maintaining robust online systems along safe and sound principles requires a comprehensive security strategy against viruses, worms, bugs, trojan horses, logic bombs, rootkits, sniffers, spyware, password crackers, backdoors, keystroke loggers and a myriad of other exploits and hacking tools out in the wild. External threats are not the only concern. Inside threats are even a greater concern because trusted employees are in a better position to exploit an organisation's security weaknesses.

4.0.5 As a result of the increasing popularity and interconnectivity of online systems, large amounts of financial transactions are moved from one place to another through public network highways and communications channels, over vast expanses of open space which are unprotected and potentially even hostile. As the data moves across these terrains, there is always the risk that it may be intercepted, altered, deleted or substituted. All these possibilities cause serious security concerns. Cryptography is the most widely established practical means of protecting data in wired or wireless communications. Encryption is a basic technique in telecommunications to attain data confidentiality and integrity.

4.0.6 To secure computer networks from end to end, it is necessary to have a multi-layered security strategy which incorporates authentication, access controls, authorisation, cryptography, data encryption, hardware crypto-modules, firewalls, intrusion detection, integrity checking, continuous surveillance, event logging, traffic analysis, security alerts, incident response procedures, vulnerability assessment, penetration testing, compliance monitoring and audit reviews. Network requirements have developed to the point where a strong security architecture needs to integrate security solutions across routers, gateways, switches, delivery channels, servers, hosts, systems, applications and databases to provide a well balanced risk control scheme.

4.0.7 With the proliferation of online systems and open networks, the challenge of administering secure access is getting more complex and difficult.

Combined this with the growing number of internal and external users, the task of managing multiple versions of user identities across multiple platforms, without lowering security is even more daunting. Cryptography is a key technology for controlling and authenticating online access to networks and systems, including virtual-private-network for establishing secure communication channels.

5.0 IDENTIFICATION AND AUTHENTICATION

5.0.1 Identification, authentication and authorization are three very important independent but related security concepts. Identification determines “who you are”, authentication tries to ascertain “you are really who you claim to be” and authorisation determines “what you are actually allowed to do”.

5.0.2 Identity management is perhaps the most difficult of the three security concepts. The security system should be able to protect authorised identities from impersonation, substitution or forgery. A user’s identity should be verified physically or through other means during account origination and confirmed before his personal profile and authentication credentials are established and stored in the system. In the authentication process the user’s identity, usually represented by a userid⁹, is verified by checking that the user has a secret which, by design, is associated with him, and which could be matched to his personal profile and authentication credentials already stored in the system. In basic terms, a userid is a claim of identity and the secret, usually a password¹⁰ or equivalent, is the evidence supporting that claim. Only after successful authentication would a user be conferred access rights to certain resources in the system for which he has been formerly authorised to access.

5.0.3 For the purpose of identification and authentication in online systems, the primary areas of security focus are:

- Identification of external and internal users.
- Access control.
- Protection of password in transit and storage.
- Protection of password during processing.
- Detection of impersonators and unauthorised logins.

⁹ Userid and username are synonymous according to the context in which they are used.

¹⁰ Passwords and PINs are synonym ous for the purpose of authentication. Passwords are usually associated with users and PINs with customers but they are commutable.

5.0.4 Most online systems still identify a user by asking for his userid which is then authenticated by verifying his password. The weakness and limitation of passwords have existed since computers were first built. Users have aggravated the problem by being careless and sloppy with their passwords which typically have very low entropy. Attackers and criminals are acutely aware of different methods of exploiting userid-password shortcomings to gain unauthorised entry into systems.

5.0.5 Strong cryptographic techniques should be used to protect passwords in all stages of creation, delivery and application. Passwords should be encrypted end-to-end through all stages of transmission, processing and storage. All encryption and decryption functions relating to passwords should be carried out in hardware security modules or similar crypto devices. Merely hashing passwords as a means of disguising them is inadequate as this method is highly vulnerable to dictionary or brute force attack. A password which is hashed also requires encryption to achieve a reasonable degree of security in transit or storage. Salting the password plus padding and iterative features would add to its protection.

5.0.6 Strong ciphers such as TripleDES, AES, RC4, IDEA, RSA and ECC should be used to protect and authenticate communication sessions or transactional dialogues between the parties interacting in an online system. The most common way to gauge the strength of a symmetric cipher is to assess its key length. But this metric is not the sole determinant of a particular cipher's robustness. The overall strength of a cipher depends on its design, construction and application. Key lengths of asymmetric ciphers are not comparable with those of symmetric ciphers. Asymmetric ciphers work on complex mathematical calculations relying on what are generally regarded as intractable mathematical problems which have no direct or simple solutions. Constant advances in computer hardware, computational number theory, cryptanalysis and brute force techniques may compel existing key lengths which are regarded as robust to be enlarged in the future. Beyond the obvious application of encryption to provide data confidentiality and integrity, cryptography also provides the basis for achieving access control and transaction authorisation. Strong cryptographic capabilities are the principal methods of achieving confidentiality, authentication, integrity and non-repudiation.

5.0.7 Password can be augmented with another form factor such as biometrics, security tokens, smart cards, USB smartkeys or digital certificates. Two factor authentication is a verification method which confirms the identity of a user based on two distinctive factors – the user's password and a physical device in the user's possession or a physical attribute of the user. To the extent that an organisation sees a need to increase online access security, it should consider the strengths and advantages of two factor authentication. The benefits of two factor authentication include its resistance to inadvertent disclosure of password,

social engineering, network sniffing, trojan horse, password cracking, keystroke capture and other forms of single-factor attack.

6.0 AUTHORISATION AND ACCOUNTABILITY

6.0.1 While authentication attempts to answer the question “are you who you claim to be?”, authorization tries to solve the question “are you allowed to access that resource?”. In most systems, authorization involves a combination of granting access rights to specific systems resources, conferring privileges as to what a user is allowed to do and deciding what actions he can take with respect to data files or transactions.

6.0.2 Each organisation should decide what rules and criteria to apply for determining each user’s level of access rights and extent of privileges. The authorisation process would usually include the requirements listed below:

- What programs or commands is the user allowed to execute.
- What system resources is the user allowed to have.
- What transactions is the user allowed to perform.
- When is the user allowed to access the system.
- What device should the user have to access the system.
- From where is the user allowed to access the system.

6.0.3 In networked systems, capturing of login sessions, transactions and other traffic is essential to establish accountability. This enables the creation of audit trails which contain information that would prevent a user from repudiating what he has done. Accountability means being able to ascertain what a user has actually done on the system.

6.0.4 A well-designed system which safeguards data integrity and processing accuracy should provide real-time event logging, violation alerts, session traffic filtering and transaction history. Transaction processing functions should be strengthened by observing the principle of segregation of duties. This means that no single individual will be allowed to initiate, authorise, process and dispose of a transaction or account on a system without the corroboration of other functions which serve to check the actions of that individual. The functions of origination, recording, reporting, approval and verification should be separated and performed by different persons according to their respective duties and responsibility levels.

7.0 TECHNOLOGY RISK GUIDELINES

7.0.1 The technology risk guidelines set out below are aimed at promoting sound processes in managing technology risks and the implementation of security practices. MAS intends to incorporate these guidelines into supervisory expectations for the purpose of assessing the adequacy of technology risk controls and security measures adopted by financial institutions. Each institution can expect that MAS will take a keen interest as to how and what extent it has achieved compliance with these guidelines¹¹.

7.1 DELINEATE RESPONSIBILITY FOR SAFETY AND SOUNDNESS

7.1.1 Financial institutions are directly responsible for the safety and soundness of the services and systems they provide to their customers and users. In this respect, they should operate and maintain robust authentication and related security functions to protect and verify their customers and users before access to their systems and services is permitted. Only then should users and customers obtain access to confidential information or perform transactions in accordance with appropriate authorisation and validation procedures.

7.1.2 The board and senior management should take steps to ensure that their institution has implemented risk management policies, security processes and authorization procedures which are appropriate for the types of computer systems, scale of operations and information assets they have. Risk control and security policies are broad statements of the organisation's approach to keeping its information assets safe. They represent high-level requirements on what risks are to be controlled and what security measures are to be implemented.

7.2 ESTABLISH RESPONSIBILITY FOR MANAGING TECHNOLOGY RISKS

7.2.1 Overall risk management policies are the responsibility of the board and senior management. Technology risks and security threats are not merely technical issues but also business and management issues. High-level risk management strategy needs to be an oversight process applied on a continuous basis. Financial institutions should develop risk management processes based on risk-weighted cost-benefit considerations, industry security best practices, corporate governance standards, regulatory guidelines and legal requirements. As no organization has an infallible security system, it should also develop rapid response capability and contingency plans in order to be prepared for new or existing risks and threats which may materialise unexpectedly.

¹¹ Financial institutions are encouraged to use their best endeavours to ensure compliance with these guidelines.

7.2.2 Without deliberately erring on either side of optimism or pessimism, the top ten risks (or some other priority enumeration) should be identified, ranked and monitored closely, with regular reporting on what actions have been taken to resolve them. These top ten risks should be updated at least quarterly and those which have been resolved should be replaced with new risks or previously lower order risks in a perpetual cycle of renewal and succession. A risk matrix which maps out the relationships of different vulnerabilities and threats would be useful in supporting this task.

7.2.3 At the executive level, a specific officer¹² should be appointed and assigned primary responsibility for information security. He should have full delegated authority to declare an emergency or shut down a system which is under attack, and determine the course of action to be taken. When encountering an attack, securing the scene and conducting an investigation is essential and should be done with great care and forensic skill.

7.3 NURTURE A RISK AWARENESS CULTURE

7.3.1 Top-level management is responsible for the protection of assets and the well-being of their employees. Through an internal security awareness program, everyone in the organisation should be encouraged to identify and report risks and threats to management so that proper assessment and appropriate actions can be taken. A proactive attitude towards risk control should be fostered. It would be difficult to control risks effectively if the prevailing culture is to deny their existence and employees are generally deterred by the “shoot the messenger” syndrome. Risk recognition, disclosure, evaluation and reporting should be conducted in a rational and analytical manner, without exaggerating nor trivialising them. Risk analysis should distinguish between the likelihood of a risk incident occurring and the possible consequences which may result from it. The latter might be so severe or calamitous that risk control strategies and recovery contingencies are necessary regardless of the probability of occurrence.

7.3.2 Financial institutions should implement internal control procedures and segregation of duties to reduce the risks of fraud, compromise of its internal functions or subversion of its operations. The reliability of systems, accuracy of processing and integrity of data depend to a large degree on the proper separation and assignment of responsibilities and duties, coupled with the

¹² This person is variously known as the chief information officer, chief technology officer, chief security officer, head of data security or chief information security officer. The role of the security officer, as approved by the Board or the CEO, should be clearly defined and articulated throughout the institution. In terms of policy development and administration, this security position provides a direct link to the Board or the CEO.

application of internal control principles. Three of the most important internal control principles¹³ for safeguarding assets and protecting data integrity are:

- Never alone principle.
- Segregation of duties principle.
- Access control principle.

7.3.3 However, these control principles are not perfect. Their main nemesis is collusion among employees or collaboration between insiders and external accomplices. Therefore, the element of independent auditing and a rigorous program of compliance checking are necessary as compensating controls.

7.4 RECTIFY THE WEAKEST SECURITY LINK

7.4.1 A security system is only as strong as its weakest link. Without a defined process of update and invigoration, security tends to obsolesce and fracture over time. The weakest security link should be identified and fixed. Then the second weakest security link should be elevated to become the first weakest which should also be fixed, and so on in a methodical manner. This continuous security enhancement process should be part of the defence-in-depth strategy.

7.4.2 The organisation should be prepared for a substantial increase in the number of viruses, worms, bugs, trojan horses and other forms of cyber attacks. Technology risks may change so abruptly or new threats emerge so suddenly that a rigid bureaucratic approach will no longer suffice for the purpose of responding swiftly with appropriate countermeasures. The organisation should also invest in early warning detection systems as well as in additional resiliency in its critical systems. This requires identification of single points of failure and other brittleness in its systems so that corrective actions can be taken.

7.5 CONDUCT VULNERABILITY AND SECURITY ASSESSMENT

7.5.1 A comprehensive evaluation of an organisation's security status should be conducted at least once a year, or more frequently if major systems changes have taken place during the year. This should include a review of its risk control processes, security standards, vulnerability assessment results, penetration test findings, configuration management practices, incident response procedures, rapid recovery capability and disaster recovery preparedness. All organisations are potential targets of hackers of varying sophistication, hues and motivations.

¹³ These three internal control principles are described in Appendix B.

7.5.2 Different organisations have different exposures to security threats. The attackers could be criminals, terrorists, hired guns, cyber vandals, black hats, disgruntled employees, aggrieved customers, hostile competitors or any adversaries from anywhere. The skill levels of these attackers vary greatly. Most attacks begin with network scanning for holes in systems, websites, applications or host installations. By scouring internet connections, protocols and network perimeters for vulnerabilities, hackers hone their skills and orchestrate their exploits. The elite hackers do not seek publicity. They value anonymity above all. They use specialised tools to gain entry and take great pains to hide their tracks. Organisations should closely evaluate these security threats and implement appropriate control countermeasures to protect their information assets.

7.6 INVEST IN SYSTEM AVAILABILITY AND INTEGRITY

7.6.1 A high level of systems availability, reliability and integrity is required for maintaining public confidence in an online network environment. All of the previous security and control components are of little value if systems services are not available when needed. Key considerations associated with maintaining high systems availability and reliability are adequate processing capacity, failsafe performance, fast response time, scalability, pre-implementation testing, system development controls, integrity verification and swift recovery capability. Financial institutions need to ensure they have ample operating resources and standby capacity in terms of hardware, software and other functional capabilities to deliver consistently reliable service. In terms of availability profile, the middleware support and backend systems are just as important as the front-end systems because of their interdependencies.

7.6.2 Institutions are expected to have in place configuration management practices, systems development controls, quality acceptance testing procedures and monitoring tools to track network traffic, response time, transaction duration, server processes, systems performance, load balancing and capacity utilisation on a continuous basis to ensure a high degree of systems uptime.

7.7 PREPARE FOR CONTINGENCIES AND DISRUPTIONS

7.7.1 As no computer system is indestructible nor infallible, contingency preparations and rapid recovery capability are necessary in order to provide for disruptive occurrences or adverse events. Recovery and business resumption priorities should be defined and contingency procedures tested so that business interruption and operating disruption arising from a serious incident could be minimised. The incident response procedures and recovery plan should be validated periodically and updated as and when major changes to the business and operating environment occur.

7.7.2 A recovery site geographically separate from the primary site should be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site. Hotsite recovery capability involving systems and data mirroring or parallel processing in synchronicity with the primary site should be established and maintained in respect of very critical systems which an organisation must absolutely have to stay in business. The required speed of recovery will depend on the criticality of resuming business operations, the type of applications to be restored and whether there are alternative ways and processing means to maintain adequate service levels to satisfy customers.

7.7.3 An alternative to a backup hotsite is to split computer operations between two separate physical sites, each with excess capacity to handle the processing requirements of the other in the event of an emergency. Both sites would have to maintain active systems capability in respect of their mutual backup and recovery arrangements. For added resilience, replicas of databases could also be kept at different backup locations to enable the primary site to switch production to these backup facilities at short notice. This geographical and operational diversity may be cost-effective and feasible only for very large institutions.

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

7.7.5 It is vital that institutions include in their incident response procedures a predetermined action plan to address public relations issues. Being able to maintain customer confidence during a period of crisis or emergency is vital to the reputation and survivability of the institution.

7.7.6 Institutions which have their networks and systems linked to dedicated service providers, such as telecommunications and utilities suppliers, should conduct bilateral or multilateral recovery testing to ensure interdependencies are not overlooked. This contingency testing should include reciprocity with other institution backup facilities.

7.8 EDUCATE CUSTOMERS ON SECURITY PRECAUTIONS

7.8.1 Financial institutions should advise their customers on how to protect the confidentiality of their information when accessing the institutions' systems, products or services. Customers play an important role in the safety of the systems they access and the devices they use.

7.8.2 Though financial institutions are duty bound to protect the confidentiality of their customer data as required by law or regulations in the jurisdictions in which they operate, end-to-end system security can only be achieved if customers also take appropriate security precautions to protect the methods and devices they use to access their online accounts, including the services and products provided by the financial institutions. Customer verification at account origination and customer authentication during online sessions are critical security techniques in preventing identity theft, impersonation, deception, forgery, fraud and other types of irregularities.

7.8.3 Institutions should provide clear and succinct information to their customers about the risks and benefits of using online, web-based and internet services. Customers should be informed clearly and precisely on their rights, obligations and responsibilities when accessing online accounts and performing online transactions. If difficulties should arise from processing errors or security breaches, customers should have already been given the necessary information to know where to obtain assistance and how to seek redress. The terms and conditions pertaining to online products and services should be readily made available to customers. 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.

7.8.4 Institutions should publish their customer privacy and security policy. Customer dispute handling, reporting and resolution procedures, including the expected timing for the institution's response, should also be clearly defined. All this information should be posted on the institution's websites. Disclosure of information should be useful and relevant in assisting the customers to make informed decisions.

7.8.5 When new operating features or requirements, particularly those relating to security, integrity and authentication, are being introduced, the institution should ensure that customers have sufficient instructions and information to be able to properly utilise them. Continual education and timely information provided to customers will help them to understand security requirements and take appropriate actions in reporting security problems.

7.8.6 To raise security awareness, institutions should provide their customers with instructions as to how to protect their personal identification numbers (PINs), passwords, access codes and other personal details. Security advice to customers on how they should protect their online access devices and computers is also necessary, including the use of firewall, intrusion detection and anti-virus protection for internet connections. Appendix D contains a list of security precautions which institutions should advise their customers to adopt.

7.9 MANAGE OUTSOURCING RISKS

7.9.1 For a variety of reasons, a growing number of institutions are turning to outsourcing their technology operations to service providers. The premise for outsourcing is generally related to the notion of cutting costs or gaining access to new technologies and technical expertise which would not otherwise be readily obtainable. Some institutions, due to size, predilection or preference, do not want to acquire, maintain or retain the necessary resources and competencies to manage and run high-tech computer operations. Whatever the reasons, it must be realised that effective utilisation of information technology is critical, for without it, many institutions would find it difficult to continue in business, let alone remain competitive.

7.9.2 The board and senior management must fully understand the risks associated with outsourcing as they cannot abdicate their responsibility for managing and controlling information technology risks. Outsourcing arrangements do not offload these risks and responsibility to the service providers. Technology risks could be very complex. They pose an even greater challenge when the technology operations of the service providers are located overseas and their outsourcing services are delivered from a foreign country. Institutions should establish a risk management program to evaluate the risks and materiality of all existing and prospective outsourcing arrangements.

7.9.3 Before a service provider is appointed, due diligence should be carried out to determine its viability, capability, reputation, track record and financial strength. The contractual terms and conditions governing the relationships, functions, obligations and responsibilities of all the contracting parties should be carefully and properly defined in written agreements. These agreements should contain provisions pertaining to service levels, performance targets, systems availability, reliability, scalability, upgrade, pricing, security, compliance, audit, inspection, dispute resolution, default, termination, early exit, contingency planning, disaster recovery preparedness, backup sites and business resumption under various disruption scenarios.

7.9.4 Outsourcing arrangements should not impede nor interfere with the regulation and inspection of financial institutions. Financial institutions should also ensure that service providers engaged by them provide regulators and authorities with access to the systems, data and facilities of the service providers for the purpose of conducting inspection, examination, compliance checking or similar tasks pursuant to regulatory requirements or other conditions. To this end, there should be provisions in outsourcing contracts for regulatory bodies to carry out any inspection, supervision or examination of a service provider's role, responsibilities, obligations, functions, data, systems and facilities.

7.9.5 The outsourcing arrangements should also take into account the need to protect the confidentiality of customer information as well as the necessity to comply with all applicable laws and regulations.

7.9.6 Given that public confidence and customer trust in financial institutions are a keystone in the stability and reputation of the financial industry, it is vital to preserve and protect the confidentiality and sanctity of customer information in the custody or possession of service providers as a result of outsourcing arrangements. For this reason more than any other, institutions should require service providers to implement security policies, procedures and controls that are at least as stringent as those they would expect for themselves. They should review and monitor the security practices and control processes of the service providers on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations of the service providers.

7.9.7 At a minimum, financial institutions should specify their requirements for confidentiality and security. The respective responsibilities of the parties for ensuring the adequacy and effectiveness of security policies and practices must be addressed, agreed and documented. Institutions have a primary duty to ensure adequate security, safety and soundness in respect of their operations. This responsibility cannot be ceded to another entity.

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

7.9.9 Institutions should also put in place a contingency plan based on credible worst-case scenarios to prepare for the possibility that their existing service providers might go out of business. The identification of viable alternatives for resuming operations is essential to provide operational continuity.

7.9.10 Outsourcing arrangements often lead to the sharing of facilities operated by the service provider. The data and systems belonging to different entities might be commingled, maintained and stored together. It is essential that commingled data and computer assets can be separated and returned to their respective owners without undue obstacles in the event of outsourcing termination.

APPENDIX A

TECHNOLOGY RISK DIMENSIONS

An ever increasing number of financial institutions and related entities are becoming dependent on the internet for their day-to-day online business transactions and communications. Most offices and households have internet access. The computer systems and networks of financial institutions form a significant part of the nation's critical infrastructure. They are also the prime targets of hackers, terrorists and criminals.

Intensity and magnitude of technology risks

As a result of the pervasiveness of computer systems connected to the internet, attacks on these systems have changed from sporadic and amateurish to omnipresent and persistent with increasing levels of sophistication, insidiousness and virulence.

Some of the factors contributing to this ominous trend are listed below.

- a) The internet is a distributed global network of computer systems with no physical, geographical, legal or national boundaries. Internet technologies and systems are often riddled with vulnerabilities which hackers can exploit faster than security experts can fix.
- b) The web is a vast playground for hackers who can obtain freely available internet exploit tools. Hacking requires little investment in effort and skill. Hackers unleash their exploits indiscriminately and persistently.
- c) Hackers are rampant. They use the internet to swap hacking tools and trade favours or services with one another. The underground currency of choice seems to be stolen credit card details.
- d) When a skilled hacker successfully develops a new hacking tool which he makes available to other hackers, computer systems which were previously secure against all hackers are no longer secure against any hackers.
- e) Criminal syndicates engage hackers to probe and attack internet computer systems. A large number of attacks are perpetrated or orchestrated by insiders or their accomplices
- f) Any hacker from anywhere at anytime can attack a computer system on the internet. Nascent vulnerabilities cleverly exploited give little advance warning.

APPENDIX B

INTERNAL CONTROL PRINCIPLES

Three of the most important internal control principles¹⁴ for systems security and data integrity 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 verified by a second person. These functions include systems initialisation, changing operating system parameters, network security configuration, access control installation, firewall and intrusion detection implementation, modifying contingency plans, invoking emergency procedures, obtaining access to backup recovery resources, creating super-user passwords and establishing master cryptographic keys.

b) Segregation of duties principle

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

c) Access control principle

Access rights and system privileges must be based on job responsibility and the necessity to have them to fulfil one's duties. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorisation should be allowed to access confidential information and use system resources solely for legitimate purposes.

¹⁴ 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.

APPENDIX C

SECURITY PRACTICES FOR FINANCIAL INSTITUTIONS

Financial institutions should adopt the following security practices:

- a) Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of enhancements, updates and patches recommended by system vendors.
- b) Change all default passwords for new systems immediately upon installation as they are mostly known by intruders at large.
- c) Install firewalls between internal and external networks as well as between geographically separate sites.
- d) Develop built-in redundancies for single points of failure which can bring down the entire network.
- e) Engage independent security specialists to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff.
- f) Conduct penetration testing at least annually.
- g) Use network scanners, intrusion detectors and security alerts.
- h) Implement anti-virus software and apply updates regularly.
- i) Establish network surveillance and security monitoring procedures.
- j) Conduct regular system and data integrity checks.
- k) Maintain access security logs and audit trails.
- l) Analyse security logs for suspicious traffic and intrusion attempts.
- m) Establish an incident management and response plan.
- n) Test the predetermined action plan relating to security incidents.
- o) Install network analysers which can assist in determining the nature of an attack and help in containing such an attack; where applicable, deploy honeypots which can act as decoys as well as capture hacking activities.

- p) Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.
- q) Maintain a rapid recovery capability.
- r) Conduct security awareness education and programs.
- s) Require frequent audits to be conducted by security professionals or internal auditors who have the requisite skills.
- t) Consider taking insurance cover for cybercrime and other insurable risks, including recovery and restitution costs.
- u) Separate physical/logical environments for systems development, testing and production.
- v) Provide separate environments for the development, testing, staging and production of internet facing web-based applications; connect only the production environment to the internet.
- w) Implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.
- x) Deploy strong cryptography and sound key management techniques to protect customer PINs and user passwords as well as other sensitive data where applicable.
- y) Implement end-to-end application layer encryption security to protect PINs and other sensitive data in communications between terminals and hosts.
- z) Turn on WEP¹⁵ 128-bit encryption in wireless local area networks and also install additional user authentication with encryption enhancements.

¹⁵ As wireless local area networks (WLAN) broadcast their radio signals, they are vulnerable to eavesdropping and other interceptions. The wired equivalent privacy (WEP) protocol based on the 802.11 wireless standard provides encryption security deemed so rudimentary that it should not be relied on for confidentiality, integrity or authentication. In most basic modes, WEP amounts to no more than window dressing in providing a brittle layer of cryptographic protection based on a static 40-bit secret key and a cleartext 24-bit initialization vector. The short key length is vulnerable to various brute force and cryptanalytic attacks. Through a crude shared-key function, the 802.11 specification provides only for the authentication of the wireless station or device, not the user. This particular authentication method is unreliable and weak. While service set identifier (SSID) and media access control (MAC) address are commonly used to improve security, they are but feeble mechanisms for authentication purposes. WEP should be enhanced with more robust encryption and user authentication solutions to ensure the integrity and confidentiality of transmitted data as well as to prevent identify theft, snooping, impersonation and unauthorized access to network resources.

APPENDIX D

SECURITY PRECAUTIONS FOR CUSTOMERS

Customers should take greater care to protect their PINs and make their own computing devices more secure when accessing their accounts or engaging in financial transactions.

To raise security awareness, financial institutions should advise their customers on the need to protect their PINs and other personal data. Security instructions should be displayed prominently in the user log-on or PIN entry web page. The following advice would be instructive in helping customers to construct robust PINs and take on better security measures:

- PIN should be at least 6 digits or 6 alphanumeric characters in length.
- PIN should not use the same digit or character more than twice.
- PIN should not be based on user-id, telephone number, birthday, other personal information or any word from a dictionary.
- PIN must be kept confidential at all times and not be divulged to anyone.
- PIN must be memorised and not be recorded anywhere.
- PIN should be changed regularly.
- The same PIN should not be used for different websites, applications or services, particularly when they relate to different entities.
- Customer should check the authenticity of the institution's website by comparing the URL and the institution's name in its digital certificate.
- Customer should check that the institution's website address changes from http:// to https:// and a security icon that looks like a lock or key appear when authentication and confidentiality are expected.
- Customer should check his account balance and transactions frequently and report any discrepancy.

- Browsers and application software should be upgraded to support SSL128-bit encryption or a higher encryption standard.

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

- Install anti-virus software and firewalls in their personal or home computers, particularly when they are linked via broadband connections, digital subscriber lines or cable modems.
- Update the anti-virus and firewall products with security patches or newer versions on a regular basis.
- Remove file and printer sharing in their computers, especially when they have internet access via cable modems, broadband connections or similar set-ups.
- Do not select the option on browsers for storing or retaining user name and password.
- Do not disclose personal, financial or credit card information to little-known or suspect websites.
- Do not open email attachments from strangers.
- Delete spam and chain emails.
- Log off the online session and turn off the computer when not in use.
- Make regular backup of critical data.
- Consider the use of encryption technology to protect highly sensitive data.
- Do not install software or run programs of unknown origin.
- Do not use a computer or a device which cannot be trusted.
- Do not use public or internet café computers to access online financial services accounts or perform financial transactions.

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.

Applicability of these Guidelines

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