



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

This module should be read in conjunction with the [Introduction](#) and with the [Glossary](#), which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To provide AIs with guidance on general principles which AIs are expected to consider in managing technology-related risks

Classification

A non-statutory guideline issued by the MA as a guidance note

Previous guidelines superseded

This is a new guideline.

Application

To all AIs

Structure

1. Introduction
 - 1.1 Terminology
 - 1.2 Legal obligations under the Seventh Schedule
 - 1.3 General framework of technology risk management
2. IT governance
 - 2.1 IT control policies
 - 2.2 Oversight and organisation of IT functions
 - 2.3 Technology risk management function
 - 2.4 Technology audits
 - 2.5 Staff competence and training
 - 2.6 IT support provided by overseas offices
3. Security management



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

- 3.1 Information classification and protection
- 3.2 Authentication and access control
- 3.3 Security administration and monitoring
- 3.4 System security
- 3.5 End-user and mobile computing
- 3.6 Physical and personnel security
- 4. System development and change management
 - 4.1 Project management
 - 4.2 Project life cycle
 - 4.3 Change management
- 5. Information processing
 - 5.1 IT operations management and support
 - 5.2 Performance monitoring and capacity planning
 - 5.3 IT facilities and equipment maintenance
 - 5.4 Disaster recovery planning
- 6. Communications networks
 - 6.1 Network management
 - 6.2 Network security and certification
 - 6.3 Wireless local area network
- 7. Management of technology service providers
 - 7.1 Management of technology outsourcing
 - 7.2 Management of other technology service providers

1. Introduction

1.1 Terminology

1.1.1 In this module terms are used with the following meanings:

- “Information technology” (IT) or “technology” encompasses automated means of originating,



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

processing, storing and communicating information, and covers recording devices, communications networks, computer systems (including hardware and software components and data) and other electronic devices;

- “IT controls” refers to internal controls over security management, system development and change management, information processing, communications networks and management of technology service providers;
- “IT governance” refers to the organisational structures and processes that align the IT mission with the institution’s strategies and business objectives, and ensure that IT resources are used effectively and technology-related risks are managed properly; and
- “Technology risk management” refers to risk management systems that enable Als to identify, measure, monitor and control their technology-related risks.

1.2 Legal obligations under the Seventh Schedule

1.2.1 Als should be aware of their legal obligations to meet the minimum authorization criteria stipulated under the Seventh Schedule to the Banking Ordinance in relation to their computer systems.

1.2.2 Specially, para. 10 of the Schedule requires Als to have adequate accounting systems and systems of control and para. 12¹ requires them to conduct their business with integrity, competence and in a manner not detrimental to the interests of depositors and potential depositors. In this connection, the MA expects Als to have in place an effective framework of technology risk management to ensure the adequacy of IT controls and quality of their computer systems.

¹ As set out in the “Guide to Authorization”, the MA will take account of the quality of an institution’s computer systems, among other factors, in considering whether the institution is conducting its business prudently and with competence.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

1.2.3 The HKMA will, in the course of its on-site examinations, off-site reviews and prudential meetings with AIs, determine as appropriate the adequacy of their technology risk management, having regard to the principles set out in this module.

1.3 General framework of technology risk management

1.3.1 This module is intended to supplement [IC-1](#) “General Risk Management Controls” by setting out general principles that the MA expects AIs to consider in their technology risk management. Further detailed guidance on managing technology-related risks of electronic banking will be covered separately in another module [TM-E-1](#) “Supervision of E-banking”.

1.3.2 As AIs increase their dependency on technology to deliver banking services, inappropriate usage of AIs’ technology resources may have significant risk implications. These include for example:

- the strategic risk resulted from poor decisions on technology-related investments;
- the operational risk caused by unauthorized access or disruptions to technology resources that support mission-critical banking services; and
- the reputation risk and the legal risk due to material security breaches or unavailability of computer systems which process customer information or transactions.

1.3.3 As set out in [IC-1](#) “General Risk Management Controls”, the Board of Directors is ultimately responsible for understanding the risks run by an AI and ensuring that they are properly managed, whereas the senior management is accountable for designing and implementing the risk management system approved by the Board² or its designated committee. To this end, the senior management should establish an effective

² For the purpose of this module, the responsibility of Board oversight of technology risk management for overseas incorporated AIs in respect of the Hong Kong operation should rest with the local senior management.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

technology risk management framework³. This normally comprises IT governance, a continuous technology risk management process, and implementation of sound practices in respect of IT controls.

- 1.3.4 The general principle is that Als are expected to implement the relevant technology risk management framework that is “fit for purpose”, i.e. commensurate with the risks associated with the types of business and operations, the technologies adopted and the overall risk management systems of individual Als. An overview of a sound framework of technology risk management is illustrated below.

³ Als may find it useful to draw other references from additional resources on technology risk management or IT controls, e.g., ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (www.iso.ch), Information Systems Audit and Control Association (www.isaca.org), IT Governance Institute (www.itgovernance.org) and Information Security Forum (www.securityforum.org).

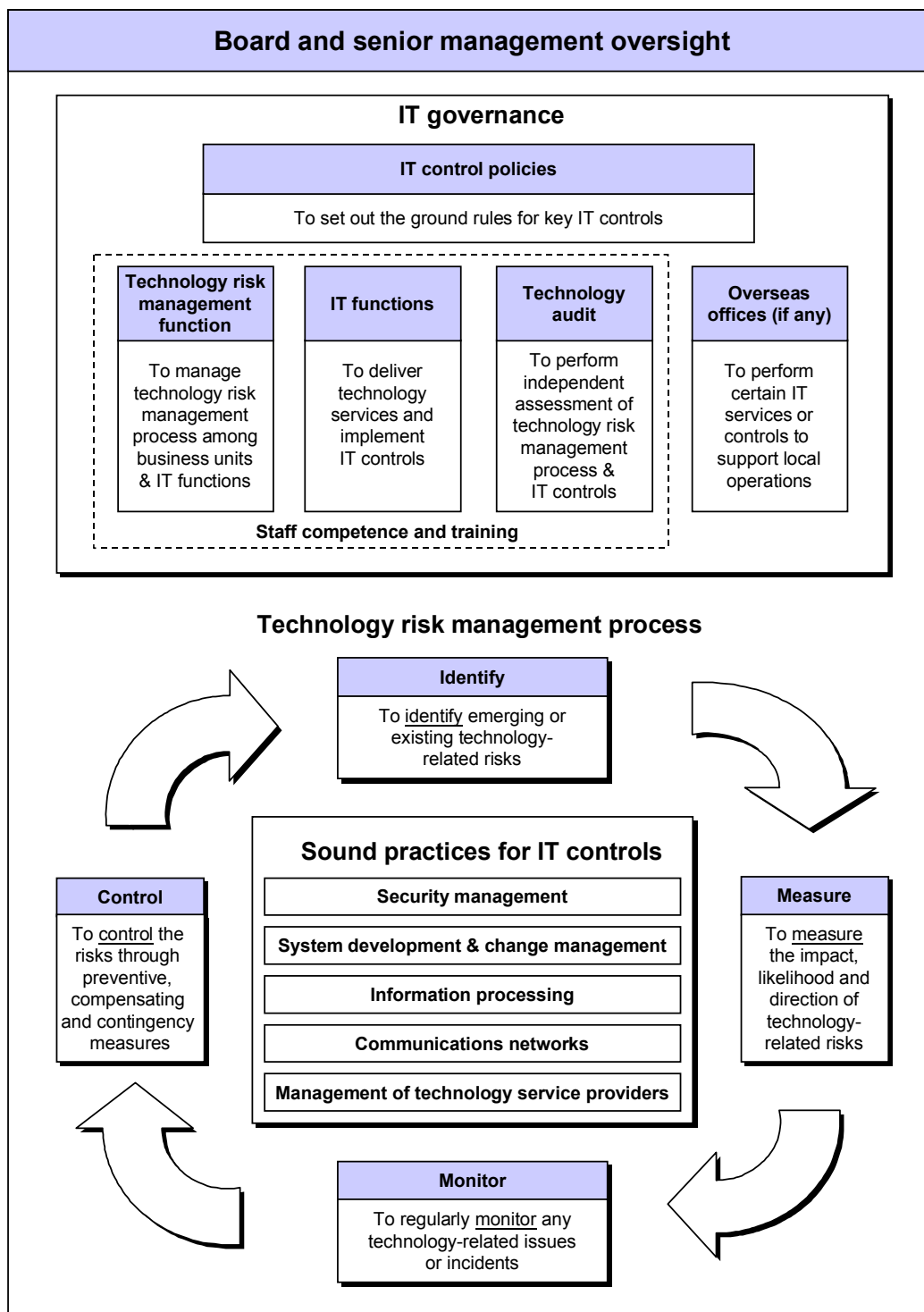


Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03





Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

2. IT governance

2.1 IT control policies

- 2.1.1 Achieving a consistent standard of sound practices for IT controls across an AI requires clear direction and commitment from the Board and senior management. In this connection, senior management, who may be assisted by a delegated sub-committee, is responsible for developing a set of IT control policies which establish the ground rules for IT controls. These policies should be formally approved by the Board or its designated committee and properly implemented among IT functions and business units.
- 2.1.2 IT control policies normally cover, at a minimum, the five aspects of IT controls mentioned in sections 3 to 7 of this module. They should be reviewed regularly, and where necessary updated to accommodate changing operating environments and technologies.
- 2.1.3 Senior management should ensure that processes used to verify compliance with IT control policies and the process for seeking appropriate approval for dispensation from IT control policies are specified clearly. Senior management should also define the consequences associated with any failure to adhere to this process. In general, the responsibility for ensuring compliance with IT control policies and the process for seeking dispensation rests with individual business units and IT functions, with the assistance of the technology risk management function (see subsection 2.3 below).
- 2.1.4 Senior management may put in place mechanisms (e.g. periodic reminders for relevant staff and policy orientation for new recruits) to promote awareness of IT control policies among relevant personnel on a regular basis.

2.2 Oversight and organisation of IT functions

- 2.2.1 Senior management should establish an effective organisation of IT functions to deliver technology services and to provide day-to-day technology support to business units. A clear IT organisation structure and related job descriptions of individual IT functions should be documented and approved by senior management.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

- 2.2.2 Proper segregation of duties⁴ within and among various IT functions is crucial for ensuring an effective IT control environment. In the event that an AI finds it difficult to segregate certain IT control responsibilities, it should put in place adequate compensating controls (e.g. peer reviews) to mitigate the associated risk.
- 2.2.3 It is recommended that AIs establish an IT planning or steering committee which oversees whether IT resources are used effectively to support business strategies. This committee should normally consist of representatives of senior management, key business units and IT functions. It should meet regularly and report to senior management, and where appropriate to the Board or its designated committee on the status of major technology-related initiatives and any material IT-related issues.
- 2.2.4 In general, the IT planning or steering committee should also be responsible for developing an IT strategy to cover longer and short-term technology-related initiatives, taking into account new business initiatives, organisational changes, technological evolution, regulatory requirements, staffing and control related issues. The IT strategy should be formally documented, endorsed by the Board or its designated committee and senior management, as well as reviewed and updated at least on an annual basis.

2.3 Technology risk management function

- 2.3.1 [IC-1](#) “General Risk Management Controls” specifies that AIs should have in place effective risk management systems and that new products and services should be subject to careful evaluation (including a detailed risk assessment) as well as a post-launch review. The same risk management controls apply to the technology risk management of AIs.
- 2.3.2 Senior management should establish clearly which function in the AI is responsible for implementing and managing the technology risk management process (the TRM function). Depending on the business and

⁴ For example, system development personnel should be prohibited from having access to production systems. The security management function should not be assigned other conflicting duties such as system development, computer operations or technical support.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

operational needs of individual AIs, the TRM function may refer to a dedicated department of an AI, or a group of departments or support units collectively performing the roles defined for this function.

2.3.3 The TRM function has a role to assist business units and IT functions in performing the technology risk management process which identifies, measures, monitors and controls technology-related risks. In addition, this function helps to ensure awareness of, and compliance with, the AI's IT control policies, and to provide support for investigation of any technology-related frauds and incidents.

2.3.4 The TRM function should formulate a formal technology risk acknowledgement and acceptance process for reviewing, evaluating and approving any major incidents of non-compliance with IT control policies. Typical reasons for such non-compliance are technology limitations (e.g. certain proprietary operating systems are only able to provide primitive password controls), business constraints (e.g. undesirable impact on customer services) and the costs outweighing the associated benefits. The process includes:

- a description of the risk being considered for acknowledgement by the owner of the risk and an assessment of the risk that is being accepted;
- identification of mitigating controls;
- formulation of a remedial plan to reduce the risk; and
- approval of the risk acknowledgement from the owner of the risk and senior management.

2.4 Technology audits

2.4.1 [IC-1](#) "General Risk Management Controls" sets out the general objective and the importance of independence and expertise of AIs' internal audit function. As regards technology audits, AIs are expected to assess periodically their technology risk management process and IT controls. To ensure adequate coverage of the IT control environment and critical computer systems, an annual technology audit plan should be developed. AIs should



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

- 2.4.2 It is recognised that the internal audit function of some Als may find it difficult to build up in-house technology audit expertise. In these circumstances, technology audit support may be supplemented by external specialists or internal technology auditors of other offices of the same banking group.

2.5 Staff competence and training

- 2.5.1 Given the rapid pace of technological development, senior management needs to ensure that staff of IT functions, the TRM function and internal technology auditors are competent and able to meet required levels of expertise and experience on an ongoing basis. It is also important to ensure that staffing levels are sufficient to handle present and expected work demands, and to cater reasonably for staff turnover.
- 2.5.2 To ensure that an adequate training programme is in place for IT personnel, it is essential to establish a process to identify any material skill gaps⁵ of staff of technology-related functions. Als may encourage and, where appropriate, facilitate their staff to acquire relevant professional qualifications, such as for those who are responsible for security management, technology risk management and technology audits.

2.6 IT support provided by overseas offices

- 2.6.1 Some Als may rely upon or work with their overseas offices (e.g. parent banks, subsidiaries, head offices or other regional offices of the same banking group) with regard to certain IT controls or support activities. Senior management should ensure that the respective responsibilities of the local and overseas offices in these areas are clearly set out in the relevant documents (e.g. policies, procedures or service agreements).

⁵ Skill gaps can be identified by evaluating the skill set of personnel against a pre-defined skill matrix which defines the required knowledge, qualifications and experience for a particular job or position.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

3. Security management

3.1 Information classification and protection

3.1.1 For each application system, Als should preferably assign an individual as the information owner⁶. The information owner normally needs to work with the TRM and IT functions to ensure confidentiality and integrity of information, and to protect the information in accordance with the level of risk present and envisaged.

3.1.2 Information can be classified into different categories according to the degree of sensitivity (e.g. highly sensitive, sensitive, internal and public) to indicate the extent of protection required. To aid the classification process, Als should ideally develop guidelines and definitions for each classification and define an appropriate set of procedures for information protection in accordance with the classification scheme. The level of detail of the information classification scheme adopted should be practicable and appropriate to Als' circumstances.

3.1.3 Protection of information confidentiality should be in place regardless of the media (including paper and electronic media) in which the information is maintained. Als should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media.

3.1.4 If cryptographic technology is used to protect the confidentiality and integrity of Als' information, Als should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include:

- provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure. In particular, the use of tamper-resistant storage is

⁶ An information owner refers to an individual who has been assigned as the business owner of an application system and is accountable for the protection of information processed by, and stored in, this application system.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

recommended to prevent the disclosure of the cryptographic keys; and

- adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys.

3.2 Authentication and access control

3.2.1 Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. Access control rules determine what application functions, system resources and data a user can access. For each application system, all users should be identified by unique user-identification codes (e.g. user IDs) with appropriate method of authentication (e.g. passwords) to ensure accountability for their activities.

3.2.2 Als should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis. Stronger authentication methods should be adopted for transactions/activities of higher risk (e.g. payment transactions, financial messages and mobile computing⁷). These usually entail multiple factors for user authentication which combine something one knows (e.g. passwords) and something one has (e.g. a smart card or hardware security tokens).

3.2.3 Extra care should be exercised when controlling the use of and access to privileged and emergency IDs⁸. The necessary control procedures include:

- granting of authorities that are strictly necessary to privileged and emergency IDs;

⁷ Mobile computing includes access to Als' computing resources from a remote location outside office premises (e.g. using notebook computers and other mobile devices).

⁸ Privileged and emergency IDs are system accounts which are created with special authorities and extended access to system resources. These IDs are normally established for system administration (i.e. system administration IDs) or for introducing emergency solutions to system problems of the production environment.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

- formal approval by appropriate personnel prior to being released for usage;
- monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);
- proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data centre); and
- change of privileged and emergency IDs' passwords immediately upon return by the requesters.

3.3 Security administration and monitoring

3.3.1 A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities. In particular, the function should cover the following areas:

- granting, changing and removing user access rights subject to proper approval of the information owners. In particular, proper procedures should be in place to ensure that a user's relevant access rights are removed when he leaves the AI or when his job responsibilities no longer require such rights;
- ensuring the performance of periodic user access re-certification (e.g. on an annual basis) that confirms whether user access rights remain appropriate and obsolete user accounts have been removed from the systems;
- reviewing security logs and violation reports in a timely manner; and
- performing incident analysis, reporting and investigation.

3.3.2 Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

of unauthorized activities being performed by the security administration function.

3.3.3 Als should establish incident response and reporting procedures to handle information security-related incidents during or outside office hours. The incident response and reporting procedures should include timely reporting to the HKMA of any confirmed IT-related fraud cases or major security breaches.

3.4 System security

3.4.1 Control procedures and baseline security requirements should be developed to safeguard application programs, operating systems, system software and databases. For example:

- access to data and programs should be controlled by appropriate methods of identification and authentication of users together with proper authorization;
- integrity of static data (e.g. system parameters) should be periodically checked to detect unauthorized changes;
- operating systems, system software, databases and servers should be securely configured to meet the intended uses with all unnecessary services and programs disabled or removed. Use of security tools should be considered to strengthen the security of critical systems and servers;
- clear responsibilities should be established to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified, assessed, tested and applied to the systems in a timely manner;
- all configurations and settings of operating systems, system software, databases and servers should be adequately documented. Periodic certifications of the security settings should be performed (e.g. by the TRM function or the technology audit function); and



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

- adequate logging and monitoring of system and user activities should be in place to detect anomalies, and the logs should be securely protected from manipulation.

3.5 End-user and mobile computing

3.5.1 While end-user computing⁹ may offer advantages (e.g. higher productivity) to an AI, it may also increase the difficulty in controlling the quality of, and access to, the system. AIs should where necessary, therefore, establish control practices and responsibilities with respect to end-user computing to cover areas such as data security, documentation, data/file storage and back-up, system recovery, audit responsibilities and training.

3.5.2 Controls over mobile computing are required to manage the risks of working in an unprotected environment. In protecting AIs' information, AIs should establish control procedures covering:

- an approval process for user requests for mobile computing;
- authentication controls for remote access to networks, host data and/or systems;
- protection (e.g. against theft and malicious software) of equipment and devices for mobile computing;
- use of data encryption software to protect sensitive information and business transactions in the mobile environment and when being transmitted; and
- back-up of data and/or systems in the mobile computing devices.

3.5.3 Software and information processing facilities are vulnerable to attacks by computer viruses and other malicious software. Procedures and responsibilities should be established to detect and prevent attacks. AIs should put in place adequate controls such as:

⁹ End-user computing is the transfer of information processing and system development capabilities from centralised data centres onto the user's desktop.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

- prohibiting the download and use of unauthorized files and software, and the access to doubtful web sites;
- installation and timely update of anti-virus software provided by reputable vendors;
- disallowing the download of executable files, and mobile codes¹⁰, especially those with known vulnerabilities (e.g. through the use of corporate firewalls and proper configuration of the browser software); and
- prompt and regular virus scanning of all computing devices and mobile users' computers, and procedures for recovering from virus infections.

3.6 Physical and personnel security

3.6.1 Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centres and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities.

3.6.2 AIs should consider fully the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of their data centres. Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could affect adversely the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a back-up generator.

¹⁰ Mobile codes refer to small programs automatically downloaded from web sites by browsers for execution.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

3.6.3 In controlling access by third-party personnel (e.g. service providers) to secure areas, proper approval of access should be required and their activities should be closely monitored. It is also important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for recruitment of permanent and temporary technology staff, and contractors.

4. System development and change management

4.1 Project management

4.1.1 Als should establish a general framework for management of major technology-related projects. This framework should, among other things, specify the project management methodology to be adopted and applied to these projects. The methodology should cover, at a minimum, allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, check points, key dependencies, quality assurance, risk assessment and approvals.

4.2 Project life cycle

4.2.1 Als should adopt and implement a full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems. In general, this should involve phases of project initiation, feasibility study, requirement definition, system design, program development, system and acceptance testing, training, implementation, operation and maintenance.

4.2.2 The project life cycle methodology should define clearly the roles and responsibilities for the project team and the deliverables from each phase. It also needs to contain a process to ensure that appropriate security requirements are identified when formulating business requirements, built during program development, tested and implemented.

4.2.3 An independent party (e.g. the quality assurance function, the TRM function or the technology audit team), which is not involved in the project development, should conduct a quality assurance review of major technology-related



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

projects, with the assistance of the legal and compliance functions if necessary. This review is to ensure compliance with the project life cycle methodology, other internal policies, control requirements, regulations and applicable laws.

- 4.2.4 A formal acceptance process should be established to ensure that only properly tested and approved systems are promoted to the production environment. System and user acceptance testing should be carried out in an environment separated from the production environment. Production data should not be used in development or acceptance testing unless the data has been de-sensitised (i.e. not disclosing personal or sensitive information) and prior approval from the information owner has been obtained. Performance testing should also be performed before newly developed systems are promoted to the production environment.
- 4.2.5 Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. As inappropriate handling of software licences may expose Als to a significant risk of patent infringement, and financial and reputation losses, Als should establish a formal software package acquisition process. In particular, the process should involve detailed evaluation of the software package (e.g. in terms of software licence, functionality, system performance and security requirements) and its supplier (e.g. its financial condition, reputation and technical capabilities).
- 4.2.6 Als should ensure that on-going maintenance and adequate support of software packages are provided by the software vendors and are specified in formal contracts. For mission-critical software packages, Als may consider including in the contracts an escrow agreement, which allows them to obtain access to the source code of the software packages under certain circumstances, such as when the software vendors cease their business.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

4.3 Change management

4.3.1 Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. An effective change management process helps to ensure the integrity and reliability of the production environment. AIs should develop a formal change management process that includes:

- classification and prioritisation of changes and determination of the impact of changes;
- roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;
- program version controls and audit trails;
- scheduling, tracking, monitoring and implementation of changes to minimise business disruption;
- a process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and
- a post implementation verification of the changes made (e.g. by checking the versions of major amendments).

4.3.2 To enable unforeseen problems to be addressed in a timely and controlled manner, AIs should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day).



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

4.3.3 Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.

5. Information processing

5.1 IT operations management and support

- 5.1.1 Management of IT functions should ideally formulate a service level agreement with business units to cover system availability and performance requirements, capacity for growth, and the level of support provided to users. The responsible IT functions should ensure that adequate procedures are in place for managing the delivery of the agreed technology support and services.
- 5.1.2 Detailed operational instructions such as computer operator tasks, and job scheduling and execution (e.g. instructions for processing information, scheduling requirements and system housekeeping activities) should be documented in an IT operations manual. The IT operations manual should also cover the procedures and requirements for on-site and off-site back-up of data and software in both the production and development environments (e.g. the frequency, scope and retention periods of back-up).
- 5.1.3 AIs should have in place a problem management system to respond promptly to IT operational incidents, to escalate reported incidents to relevant IT management staff and to record, analyse and keep track of all these incidents until rectification of the incidents. A helpdesk function can be set up to provide front-line support to users on all technology-related problems and to relay the problems to relevant IT functions for investigation and resolution.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

5.2 Performance monitoring and capacity planning

- 5.2.1 Als should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable problems to be identified and corrected before they affect system performance. This process should help the preparation of workload forecasts to identify trends and to provide information needed for the capacity plan, taking into account planned business initiatives.
- 5.2.2 Capacity planning should be extended to cover back-up systems and related facilities in addition to the production environment.

5.3 IT facilities and equipment maintenance

- 5.3.1 To ensure the continued availability of Als' technology-related services, Als should maintain and service IT facilities and equipment (e.g. computer hardware, network devices, electrical power distribution, UPS and air-conditioning units) in accordance with the industry practice, and suppliers' recommended service intervals and specifications. Proper record keeping (including suspected or actual faults, and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance. A hardware and facility inventory should be kept to control and track all hardware and software purchased and leased. These records can also be used for regular inventory taking.

5.4 Disaster recovery planning

- 5.4.1 Als should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. Please refer to [TM-G-2](#) "Business Continuity Planning" on how to develop detailed recovery procedures of application systems and technology services, and ensure adequate insurance coverage of IT resources.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

6. Communications networks

6.1 Network management

- 6.1.1 Communications networks convey information and provide a channel of access to application systems and systems resources. Given their technical complexity, communications networks can be highly vulnerable to disruption and abuse. Safeguarding communications networks requires robust network design, well-defined network services and sound discipline to be observed in managing networks.
- 6.1.2 Overall responsibility for network management should be clearly assigned to individuals who are equipped with the know-how, skills and resources to fulfil their duties. Network standards, design, diagrams and operating procedures should be formally documented, kept up-to-date, communicated to all relevant network staff and reviewed periodically.
- 6.1.3 Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimised by automatic re-routing of communications through alternate routes should critical nodes or links fail (e.g. routing critical links to more than one external exchange or switching centre, and pre-arranging services with alternate telecommunications service providers).
- 6.1.4 The network should be monitored on a continuous basis. This would reduce the likelihood of network traffic overload and detect network intrusions. Monitoring activities include:
- monitoring network services and performance against pre-defined targets;
 - reviewing volumes of network traffic, utilisation of network facilities and any potential bottlenecks or overloads; and
 - detection of unusual network activities based on common attack characteristics.
- 6.1.5 Powerful network analysis and monitoring tools, such as protocol analysers, network scanning and sniffer tools, are normally used for monitoring network performance



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage (e.g. viewing of unencrypted sensitive information). The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures.

6.2 Network security and certification

6.2.1 To prevent insecure connections to an AI's network, procedures concerning the use of networks and network services need to be established and enforced. These should cover:

- the available networks and network services;
- authorization procedures for determining who is allowed to access particular networks and network services; and
- controls and procedures to protect access to network access points, network connections and network services.

6.2.2 AIs should consider segregating internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. For instance, the production systems should be located in dedicated network segments separated from other segments so that production network traffic is segregated from other traffic (e.g. connections to the internet, extranet connections to external parties and market data feeds). Sensitive data traffic between different network segments should be properly controlled and protected from being tampered with.

6.2.3 Regular reviews of the security parameter settings of network devices such as routers, firewalls and network servers are required to ensure that they remain current. Audit trails of daily activities in critical network devices should be maintained and reviewed regularly. Network operational personnel should be alerted on a real-time basis to potential security breaches.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

6.2.4 Network certification¹¹ should be conducted when requesting local area network (LAN)/wide area network (WAN) additions or changes to Als' corporate network. The additions or changes cover dial-in/out ports, switches, terminal servers, gateways/servers, routers, extranets and the public internet. The network certification process includes gathering data about the network environment, analysing any points of vulnerability and associated controls, and documenting whether approval is given or what additional controls are required for approval of connectivity.

6.3 Wireless local area network

6.3.1 If wireless local area networks (WLANs) are to be deployed, Als should develop policies and procedures for approval, installation, operation and administration of WLANs. A risk assessment process for evaluating the sensitivity of information to be accessible via a WLAN should be formulated before a WLAN can be implemented. Als should also develop a standard security configuration for WLAN products and follow the network certification process to ensure that WLANs are implemented in a secure manner so that they do not expose the corporate network to unmanaged risks.

6.3.2 Additional security measures may be needed between the wireless workstations and the wired network to provide stronger encryption and mutual authentication. WLANs should be segregated from the corporate network (e.g. by firewalls) to prevent any unauthorized access to the corporate network via WLANs.

7. Management of technology service providers

7.1 Management of technology outsourcing

7.1.1 While Als are expected to take into account the general guidance specified in [SA-2](#) "Outsourcing" when managing

¹¹ Network certification refers to an assessment process which aims to ensure that additions or changes to network devices and infrastructure do not impose points of vulnerability to other parts of the corporate network. Network certification may form part of the network change management process.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

technology outsourcing¹², they should also have regard to the following controls:

- technology service providers should have sufficient resources and expertise to comply with the substance of the AIs' IT control policies;
- in case of outsourcing of critical technology services (e.g. data centre operations), AIs are expected to commission a detailed assessment of the technology service provider's IT control environment. The assessment should ideally be conducted by a party independent of the service provider. The independent assessment report should set out clearly the objectives, scope and results of the assessment and should be provided to the HKMA for reference;
- the outsourcing agreement should specify clearly, among other things, the performance standards and other obligations¹³ of the technology service provider, and the issue of software and hardware ownership. As technology service providers may further sub-contract their services to other parties, AIs should consider including a notification or an approval requirement for significant sub-contracting of services and a provision that the original technology service provider is still responsible for its sub-contracted services;
- further to the regular monitoring activities set out in [SA-2](#) "Outsourcing", AIs should conduct an annual assessment to confirm the adequacy of the IT control environment of the provider of critical technology services;

¹² In line with [SA-2](#) "Outsourcing", "technology outsourcing" refers to an arrangement under which another party undertakes to provide to an AI a technology service previously carried out by the AI itself or a new technology service to be launched by the AI. Technology outsourcing can be to a service provider in Hong Kong or overseas and the service provider may be a unit of the same AI (e.g. the head office or an overseas branch), an affiliated company of the AI's group or an independent third party.

¹³ These may include the obligations of the technology service provider in ensuring confidentiality of the AI's information obtained by the provider's staff or agents and complying with the AI's relevant IT control policies and procedures.



Supervisory Policy Manual

TM-G-1

General Principles for Technology Risk Management

V.1 – 24.06.03

- Als should try to avoid placing excessive reliance on a single outside service provider in providing critical technology services; and
- Als should develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider¹⁴. This may include an exit management plan and identification of additional or alternate technology service providers for such support and services.

7.2 Management of other technology service providers

7.2.1 Apart from technology outsourcing, Als may rely on some outside technology service providers in the provision of technology-related support and services (e.g. telecommunications and network operators). Als should have in place guidelines on how to manage different kinds of major outside technology service providers. Similar to the general principles set out in [SA-2](#) “Outsourcing” and subsection 7.1 above, the guidelines may need to cover the selection process of service providers, the process for approving material exceptions, and the need to avoid over-reliance upon a single technology service provider in critical technology services.

Contents	Glossary	Home	Introduction
--------------------------	--------------------------	----------------------	------------------------------

¹⁴ The service provider may become insolvent or have other difficulty to continue provision of the services and support.