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 set out the HKMA's approach to the supervision of AIs' electronic banking (e-banking) services and to provide AIs with guidance on general principles for risk management of e-banking

Classification

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

Previous guidelines superseded

Guideline 15.1 "Electronic Banking" dated 07.07.97

Guideline 15.1.1 "Security of Banking Transactions over the Internet" dated 25.11.97

Guideline 15.3 "Public Key Infrastructure and Legal Environment for Development of Internet Banking" dated 07.10.98

Circular "Guidance Note on Management of Security Risks in Electronic Banking Services" dated 06.07.00

Circular "Guidance Note on Independent Assessment of Security Aspects of Transactional E-banking Services" dated 26.09.00

Circular "Overseas Fraud Cases involving Fake E-mails or Websites" dated 19.05.03

Application

To all AIs

Structure

1. Introduction

1.1 Terminology

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

- "Demilitarised zone" (or DMZ) refers to a network segment inserted between a trusted internal network and an external network such as the internet, in order to prevent parties of the external network from getting direct access to the trusted internal network, and vice versa;
- "Electronic banking" (or e-banking) refers to banking services involving the transmission of confidential customer information (including transactions) through the internet[1]. For the purpose of this module, e-banking covers services for personal, corporate and institutional customers;
- "Firewall" refers to devices (with hardware and software) that can examine the packets, pattern of packets and network services flowing between two or more networks, such as the trusted internal networks, the DMZ and the internet so as to determine whether the packets and network services should be given access into, or allowed to move between, these networks;
- "Intrusion Detection System" (or IDS) refers to computer systems which collect relevant information from host computers, servers or networks for detecting signs of intrusion and misuse of computer resources, and alerting relevant personnel to these activities; and

[1] E-banking does not cover (i) automated teller machines or self-service machines connected through private networks; (ii) phone banking; (iii) personal computer (PC) banking connected through dial-up telephone lines; and (iv) mobile banking services that do not involve connection through the internet.

- "Routers" refer to network devices which are used to direct network traffic between networks. Routers are often used as security devices on computer networks to allow only certain types of packets and network services from a network to enter the other network.

1.2 Background

1.2.1 The development of e-banking services brings risks as well as benefits to AIs. While the types of risks arising from e-banking are generally not new to an AI, the characteristics of e-banking may shift the AI's risk profiles to some degree and create new risk management challenges. In particular:

- the internet is a global and open network accessible from anywhere in the world by unknown parties. The security of the internet and devices used by customers to access e-banking are outside AIs' direct control. It therefore adds to AIs' operational risk in respect of security breaches and service interruptions;
- the operational risk and reputation risk of AIs may be increased as the growing dependence on technology and the technical complexity of e-banking may lead to more reliance upon outside technology service providers such as telecommunications operators, and application and security vendors;
- it may be a strategic challenge for AIs to determine whether and when specific e-banking services should be introduced. This is particularly relevant if it is unclear whether the benefits of offering or maintaining the services will outweigh the initial investment and the ongoing expenses needed to maintain an appropriate level of security of the services; and
- e-banking may expose AIs to reputation and legal risks if overseas authorities regard the services as targeting at overseas residents and requiring authorization in their jurisdictions.

2. Supervisory approach

2.1 Supervisory objective

2.1.1 The HKMA's supervisory objective is to establish and maintain a safe and sound environment for the development of e-banking in Hong Kong without standing in the way of progress.

2.1.2 To achieve this objective, the HKMA believes that maintaining technological neutrality is crucial for allowing AIs to have the flexibility to choose and implement technologies that are appropriate to their e-banking services. Setting absolute risk management requirements or rigid technological standards in the area of e-banking is impractical and counter-productive.

2.1.3 The general principle is that AIs are expected to implement the relevant risk management controls that are "fit for purpose", i.e. commensurate with the risks associated with the types and amounts of transactions allowed, the electronic delivery channels adopted and the risk management systems of individual AIs.

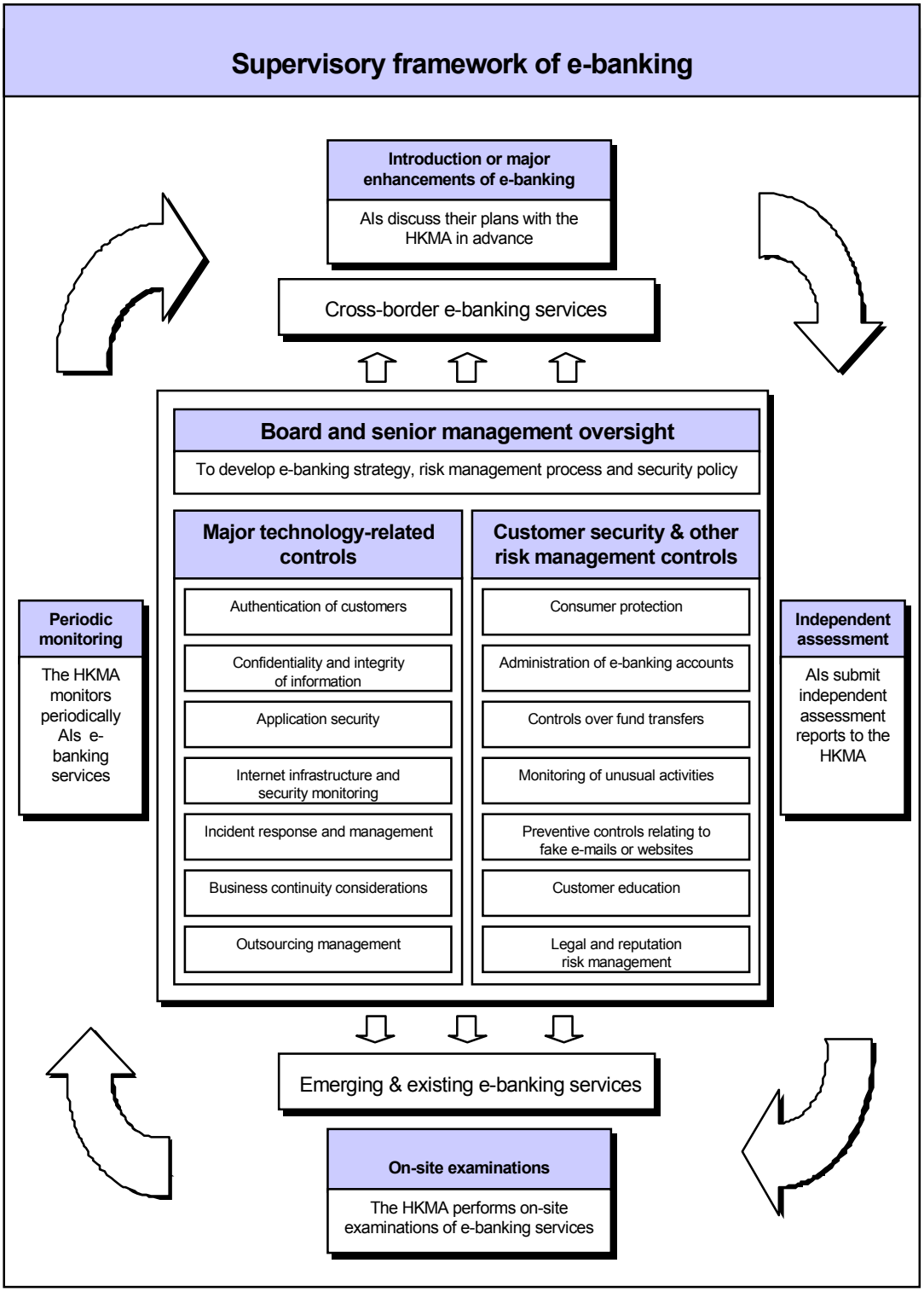
2.1.4 In developing this module, the HKMA has taken into consideration supervisory approach and guidance of the international regulatory community, particularly those recommended by the Basel Committee on Banking Supervision[2]. However, it should be emphasised that this module is not intended to prescribe uniform or all-inclusive principles and practices in managing the risks for all kinds of e-banking services.

2.2 Supervisory framework of e-banking

2.2.1 In line with the risk-based supervisory methodology, the HKMA's supervisory framework of e-banking aims to provide an appropriate level of continuous supervision of AIs' e-banking activities. This supervisory framework comprises an effective supervisory approach to e-banking, which is conducted in a continuing cycle, in

[2] The Basel Committee on Banking Supervision has issued a number of papers on e-banking, in particular: "Risk Management Principles for Electronic Banking" of July 2003 (http://www.bis.org/publ/bcbs98.htm) and "Management and Supervision of Cross-Border Electronic Banking Activities" of July 2003 (http://www.bis.org/publ/bcbs99.htm).

ensuring the adequacy of AIs' management oversight and risk management of their e-banking services (see sections 3 to 5 below). An overview of the supervisory framework of e-banking is illustrated below.


Supervisory framework of e-banking
Introduction or major enhancements of e-banking
AIs discuss their plans with the HKMA in advance
Cross-border e-banking services
Board and senior management oversight
To develop e-banking strategy, risk management process and security policy
Major technology-related controls
Authentication of customers
Confidentiality and integrity of information
Application security
Internet infrastructure and security monitoring
Incident response and management
Business continuity considerations
Outsourcing management
Customer security & other risk management controls
Consumer protection
Administration of e-banking accounts
Controls over fund transfers
Monitoring of unusual activities
Preventive controls relating to fake e-mails or websites
Customer education
Legal and reputation risk management
Periodic monitoring
The HKMA monitors periodically AIs e-banking services
Independent assessment
AIs submit independent assessment reports to the HKMA
Emerging & existing e-banking services
On-site examinations
The HKMA performs on-site examinations of e-banking services

2.3 Introduction or major enhancements of e-banking services

2.3.1 Although AIs do not need to seek formal approval from the HKMA to offer new e-banking services, AIs should discuss their plans with the HKMA in advance before launching such new services. They should also discuss with the HKMA their plans to introduce major enhancements[3] to existing services. In general, the discussion should satisfy the HKMA that the following issues are properly addressed:

- Board and senior management oversight (see section 3);
- major technology-related controls relevant to e-banking (see section 4) and, in particular, the result of an independent assessment of the service (see also subsection 2.4 below);
- customer security and other risk management controls (see section 5) and, particularly, whether the terms and conditions of the service comply with the Code of Banking Practice if the service is offered to personal customers; and
- any other relevant supervisory issues related to activities such as outsourcing (see SA-2 "Outsourcing"), conducting certain regulated activities specified in the Securities and Futures Ordinance through the internet (see SB-1 "Supervision of Regulated Activities of SFC-Registered Authorized Institutions") and cross-border e-banking activities (see subsection 2.6 below).

2.4 Independent assessments

2.4.1 The senior management of an AI are required to appoint trusted independent experts (the "assessor(s)") to carry out an independent assessment before the launch of new e-banking services or major enhancements to existing services. The scope and items to be reported in the independent assessment should cover, at a minimum, the areas specified in Annex A. The

[3] These refer to major service enhancements or changes in technologies which have material risk implications for the AI concerned or its customers.

independent assessment report should be submitted to the HKMA for reference. If the AI has engaged different parties (e.g. internal auditors, external auditors or security consultants) to conduct separate independent assessments on different aspects of its e-banking services, it may submit either a combined report or all relevant reports separately to the HKMA.

2.4.2 Thereafter, AIs should perform a formal risk assessment, at least on an annual basis, to determine if any further independent assessments are necessary and if so the frequency and scope of such independent assessments. The risk assessment should take into account substantial changes to the risk profile of services being provided, significant modifications of an AI's internet infrastructure (including system patches) and e-banking applications, material system vulnerabilities or major security breaches. The reports of such independent assessments will be, where appropriate, reviewed as part of the HKMA's on-site examinations and off-site reviews.

2.4.3 An assessor should have, and be able to demonstrate, the necessary expertise in the field to perform an independent assessment. To ensure impartiality, the assessor should be independent from the parties that develop, implement or operate the services and not be involved in the operations to be reviewed or in selecting or implementing the relevant control measures to be reviewed. The assessor should be able to report its findings freely and directly to the senior management of the AI as appropriate.

2.4.4 As long as the assessor meets the above requirements on expertise and independence, the assessor can be an external party (e.g. an external auditor or third-party security consultant) or an AI's internal staff (e.g. internal auditors).

2.5 On-site examinations and other monitoring process

2.5.1 The HKMA will, in the course of its on-site examinations and off-site reviews, determine as appropriate the adequacy of AIs' risk management of e-banking services, having regard to the principles set out in this module (see sections 3 to 5 below).

2.5.2 AIs should report promptly to the HKMA of any suspected or confirmed fraud cases relating to e-banking, major security breaches, any material service interruption or other significant issues related to their e-banking services. The HKMA may also implement other monitoring process (e.g. supervisory control self-assessment) to facilitate its ongoing supervision of e-banking.

2.6 Supervision of cross-border e-banking services

2.6.1 The HKMA observes the guidance of the Basel Committee's Concordat[4], its later supplements and the paper "Management and Supervision of Cross-Border Electronic Banking Activities" of June 2003 for supervisory cooperation and sharing of information between home and host supervisors in respect of supervision of cross-border e-banking services.

2.6.2 In general, a locally incorporated AI planning to introduce a cross-border e-banking service to another jurisdiction in which it does not have a physical presence should discuss with the HKMA in advance. The HKMA needs to be satisfied that the AI has conducted adequate due diligence (e.g. through AIs' consultation with the appropriate local supervisors) to determine the applicability of laws, regulations and supervisory standards in the foreign jurisdiction. Further, AIs should have an effective and on-going risk management process for its cross-border e-banking activities.

3. Board and senior management oversight

3.1 Planning and organisation

3.1.1 The unique characteristics and relatively high up-front investment of the e-banking service may have material risk implications for AIs. In this connection, the HKMA expects the Board[5] or its designated committee, and

[4] See "Principles for the Supervision of Bank's Foreign Establishments", generally known as the "Concordat", issued by the Basel Committee on Banking Supervision in May 1983.

[5] For the purpose of this module, the responsibility for the oversight of e-banking in respect of the Hong Kong operations of an overseas incorporated AI would rest with its local management.

senior management of AIs to ensure that the e-banking service that is new to their AI should be subject to careful evaluation (see also IC-1 "General Risk Management Controls" on new products and services).

3.1.2 The objective of the evaluation is to ensure that the Board or its designated committee, and senior management fully understand the risk characteristics and that there are adequate staffing, expertise, technology and financial resources to launch and maintain the service.

3.1.3 A new e-banking service that could have a significant impact on an AI's risk profile should be brought to the attention of the Board or its designated committee. In general, the Board or its designated committee should ensure that their AI does not offer that service unless it has the required expertise to exercise effective risk management oversight.

3.1.4 The Board or its designated committee, and senior management should also ensure that a formal business strategy for introducing a new e-banking service is in place. Moreover, the e-banking strategy should form part of the AI's overall business strategy.

3.2 Risk management process

3.2.1 The Board or its designated committee should ensure that the risk management of e-banking is an integral part of the AI's risk management system (see IC-1 "General Risk Management Controls" and TM-G-1 "General Principles for Technology Risk Management"). As a result, the applicable risk management policies and processes, and the relevant internal controls and audits as required in the AI's risk management system should be enforced and carried out as appropriate for the AI's e-banking services.

3.2.2 In addition, the Board or its designated committee should ensure that the AI's risk management controls and systems are modified and enhanced as necessary to cope with the risk management issues associated with e-banking. The e-banking-related risk management controls normally cover, at a minimum, the controls mentioned in sections 4 and 5 of this module.

3.3 Formulation of information security policy

3.3.1 The senior management should ensure that the AI develops and maintains, on a regular basis, comprehensive information security policies relating to its e-banking services. The policies should be approved and issued by the senior management. The documents should set forth the policies, procedures and controls to safeguard the AIs' operations against security breaches and intrusions, define individual responsibilities, and describe enforcement and disciplinary actions for non-compliance.

3.3.2 Apart from the issuance and maintenance of information security policies, the senior management should also promote a security culture within the institution by demonstrating their commitment to high standards of information security in relation to e-banking, and widely communicating this to all relevant staff.

4. Major technology-related controls relevant to e-banking

4.1 Authentication of customers

4.1.1 AIs should select reliable and effective authentication techniques to validate the identity and authority of their e-banking customers. Customer authentication is usually stronger when combining the following two factors:

- something a customer knows (e.g. user IDs and passwords); and
- something a customer has (e.g. one-time passwords[6] generated by a security token or AIs' security systems, a hardware electronic key, , or the customer's private key[7] stored in a smart card or other devices in the customer's possession).

[6] "One-time password" is a password that is valid for authentication only for a single access attempt or a limited period of time (e.g. around sixty seconds) so that even if this one-time password is captured by a hacker, the password cannot be reused for subsequent authentication.

[7] In simple terms, "private key" is a secret cryptographic key that is provided only to the customer for authenticating the customer's identity through public key cryptography.

4.1.2 AIs need to evaluate carefully whether a particular authentication method is sufficiently mature, and to what extent the method remains secure even if a customer's PC is compromised, e.g. by a Trojan horse program[8]. In general, the HKMA expects AIs to employ stronger customer authentication such as a combination of the above factors[9] for authenticating their customers' transactions with higher risk (e.g. unregistered third-party transfers and large-value transactions for corporate or institutional customers).

4.1.3 If AIs determine to use only user IDs and passwords to authenticate their e-banking customers after careful consideration of other relevant factors, they should implement adequate customer security measures to protect their customers' passwords and to adopt an effective monitoring mechanism to detect any unusual activities (see section 5 below).

4.1.4 Other than measures for authentication of customers, AIs should also implement appropriate means (e.g. installing digital certificates and related keys on their e-banking servers) for customers to validate the identity and genuineness of their websites (see also para. 5.5.1 below).

4.2 Confidentiality and integrity of information

4.2.1 E-banking services entail transmission of sensitive information (e.g. e-banking passwords) over the internet and AIs' internal networks. AIs should therefore implement appropriate techniques to maintain confidentiality and integrity of sensitive information while

[8] A Trojan horse is a computer program in which a harmful code is contained inside an apparently harmless program (e.g. a computer game). Trojan horses can infect a PC in circumstances such as when the attacker exploits the vulnerabilities of certain operating systems, and the victim opens contaminated e-mail attachments or visits malicious websites. Trojan horses can be used to capture screen displays and keystrokes, to steal information stored in, or to take over the control of, victims' PCs.

[9] For instance, employment of a two-factor authentication such as a combination of passwords and digital certificates will provide stronger customer authentication for higher risk transactions than a single factor authentication. AIs may consider exploring the feasibility of using the public key infrastructure developed and digital certificates issued locally (e.g. by Hongkong Post) to strengthen their customer authentication process.

it is in passage over the internal and external networks, and also, when it is stored inside AIs' internal systems.

4.2.2 Cryptographic technologies can be used to protect the confidentiality and integrity of sensitive information. AIs should choose cryptographic technologies that are appropriate to the sensitivity and importance of information and the extent of protection needed. AIs are recommended to adopt cryptographic technologies that make use of internationally recognised cryptographic algorithms where the strengths of the algorithms have been subjected to extensive tests. AIs should implement sound key management practices to safeguard their cryptographic keys.

4.2.3 AIs should consider the need to apply strong "end-to-end" encryption to the transmission of sensitive information (e.g. e-banking passwords) so that it is encrypted all the way between customers' devices and AIs' trusted internal networks. This would help reduce the risk of sensitive information being compromised if AIs' web servers[10] or DMZ were penetrated.

4.2.4 If the technology selected by AIs does not allow "end-to-end" encryption and there is a decryption process at some point between the customers' devices and institution's trusted internal networks, AIs should take appropriate measures[11] to protect the sensitive information.

4.2.5 In addition to the cryptographic techniques, AIs should also implement other controls necessary to maintain confidentiality and integrity of information processed by their e-banking systems. For example, these include:

- checks and controls incorporated in the application systems so as to reconcile data file balances after transaction updates and to check the integrity of data transmitted between different systems;

[10] A web server is a computer dedicated to connect with the internet and serves the files that form the web page for access by any users on the internet.

[11] One of the possible measures is that any cryptographic process (e.g. decryption and encryption) should be performed in a secure environment that is highly tamper-resistant.

- segregation of e-banking transaction processing and monitoring functions so that no single individual staff will be allowed to initiate, authorize, process and dispose of an e-banking transaction or account without the collaboration of other functions which serve to check the actions of that individual; and
- monitoring of unusual activities including any e-banking transactions or records being tampered with (see subsection 5.4 below).

4.3 Application security

4.3.1 Inadequate application security in e-banking systems increases the risk of successful penetration or security attacks. As a result, AIs should ensure an appropriate level of application security in respect of their e-banking systems having regard to the following sound practices[12]:

- when AIs select system development tools or programming languages for developing e-banking application systems, they should evaluate the security features that can be provided by different tools or languages to ensure that effective application security can be implemented. In the case of selecting a third-party developed e-banking system, AIs should take into account the appropriateness of the application security of the system;
- comprehensive and effective validation of input parameters (including user-supplied data and database queries that may be submitted by the users' computers) should be performed on server side. This prevents intentional invalid input parameters from being processed by the e-banking system that may result in unauthorized access to data, execution of commands embedded in the parameters or a buffer overflow

[12] AIs may find it useful to draw other references on application security, e.g. The Open Web Application Security Project (www.owasp.org) and the SANS (SysAdmin, Audit, Network, Security) Institute (www.sans.org).

attack[13]. Moreover, e-banking systems should operate with the least possible system privileges;

- error messages generated by the application system for e-banking customers should not reveal details of the system which are sensitive. Errors should be appropriately logged. Similarly, the HTML[14] source code on the production web server should not contain sensitive information such as any references or comments that relate to the design features of the web application code;
- the mechanism for managing an active e-banking session should be secure. For example, a session should be terminated after a defined period of inactivity. Web pages containing sensitive information should not be cached in the temporary files of browsers;
- the application should ideally prohibit the customers' browsers from memorising or displaying the e-banking user IDs and passwords previously entered by customers and the e-banking web pages previously accessed by customers;
- when a known vulnerability related to the e-banking application system is identified or reported, a review of the relevant program source code should be conducted as appropriate to ensure that the vulnerability is appropriately addressed. A security standard may be defined for the purpose of system development and code review. For third-party developed systems, the patches provided by vendors from time to time should be appropriately applied to these systems;

---

[13] A buffer overflow attack aims at sloppily written programs which can read in more input data than it is designed to handle and causes parts of the computer memory being overwritten by the accepted data. These excessive input data could be manipulated to result in crashing of programs or execution of some sensitive instructions for unauthorized purposes in the targeted computer.

[14] HTML refers to the Hypertext Markup Language, which is a standardised web page description language for creating web pages.

- hidden directories that contain administrative pages or sensitive information of the web site should either be removed from the production web server or protected by effective authentication and access control mechanisms. Back-up files and common files[15] should be removed from the production servers or the structure of file directories to prevent access by unauthorized users; and
- a periodic security review of the structure of file directories and access controls of the files is necessary to ensure that all sensitive files are appropriately protected and not exposed through the web applications.

4.4 Internet infrastructure and security monitoring

4.4.1 AIs should establish an appropriate operating environment that supports and protects their e-banking systems. An appropriate operating environment normally comprises a secure internet infrastructure (including the design of the DMZ and configuration of the servers, IDSs, firewalls and routers) and adequate security measures for the internal networks and network connections to external parties (see also TM-G-1 "General Principles for Technology Risk Management" on network security and certification).

4.4.2 AIs should proactively monitor their e-banking systems and internet infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions or weaknesses[16]. Comprehensive audit logs and appropriate real-time security alerts (e.g., IDS alerts) should be produced for timely review by responsible personnel or teams. Audit logs should be protected against unauthorized manipulation and retained for a reasonable period (e.g. three months) to facilitate any

[15] Back-up files and common files may contain file logs, pages, scripts or old versions of the website. The attacker normally searches through every file directory for these back-up and common folder names and file extension to obtain sensitive information of the site.

[16] In general, AIs are expected to monitor, at least on a daily basis, the security vulnerabilities and computer virus alerts published by relevant sources such as the Hong Kong Computer Emergency Response Team Coordination Centre (www.hkcert.org), anti-virus vendors and system vendors.

fraud investigation and any dispute resolution if necessary.

4.4.3 AIs should refer to Annex B on the sound practices for designing, establishing and monitoring their internet infrastructure.

4.5 Incident response and management

4.5.1 AIs should put in place formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, frauds or service interruptions of their e-banking services during or outside office hours. The incident response and management procedures should allow AIs:

- to find out quickly the origin of the incident (especially whether or not it arises from weaknesses in the AI's own security controls or operating environment);
- to assess the potential scale and impact of the incident;
- to escalate promptly the incident to the senior management if the incident may result in reputation damage or material financial loss;
- to notify promptly the affected customers where appropriate;
- to contain the damage to the AI's assets, data, reputation and, in particular, their customers;
- to collect and preserve forensic evidence as appropriate to facilitate the subsequent investigation and prosecution of suspects and intruders if necessary; and
- to perform a review of the incident.

4.5.2 A communication strategy should be developed to adequately address the concerns of external parties (e.g. customers, media and business partners) that may arise due to the incident.

4.5.3 An incident response team, which can be the technology risk management function or may comprise team members from relevant functions, should be established to manage and respond to the incident in accordance with the above procedures. The team should be given

the authority to act in an emergency and sufficiently trained in using IDSs, interpreting the significance of related data in audit logs, and determining the appropriate action to be taken (e.g. blocking particular network traffic or switching off some of the services).

4.6 Business continuity considerations

4.6.1 E-banking services should be delivered on a continuous basis with a reasonable system response time in accordance with the AI's terms and conditions and anticipated customer expectations. The availability of critical e-banking services is highly dependent upon their capacity (e.g. including the capacity of e-banking systems, associated networks and interfaces with the internal systems), ability to switch to back-up systems which are protected against similar disruptions and the effectiveness of the alternate channels for the e-banking services.

4.6.2 Performance criteria for each critical e-banking service should be established, and the service level should be monitored against these criteria. Appropriate measures should be taken to ensure that e-banking systems and the interfaces with the internal systems can handle the projected transaction volume and future growth in e-banking.

4.6.3 While AIs are expected to take into account the general guidance specified in TM-G-1 "General Principles for Technology Risk Management" and TM-G-2 "Business Continuity Planning" when developing their e-banking business continuity plan (BCP), they should also have regard to the following practices:

- the e-banking BCP should set out a process for resuming or replacing e-banking processing capabilities, and reconstructing transactions if necessary, in the event of a business disruption;
- the e-banking BCP should be able to address any dependency on outside service providers (e.g. internet service providers); and
- if an alternate service delivery channel is used for contingency arrangement of a critical e-banking service, AIs need to ensure that the alternate service delivery channel can provide an

appropriate level of continuous service to its customers, taking into account customers' demand and expectations.

4.7 Outsourcing management

4.7.1 Given the technical complexity and the global nature of the internet, some AIs may rely on another unit of the same banking group (e.g. the head office) or outside service providers to operate and maintain IT systems or business processes that support their e-banking services. In these cases, AIs should have regard to the controls specified for management of technology outsourcing in TM-G-1 "General Principles for Technology Risk Management" and SA-2 "Outsourcing".

4.7.2 AIs should perform due diligence regularly to evaluate the financial soundness and ability of outside service providers to maintain an adequate level of security and to keep abreast of rapidly changing technologies. The HKMA also expects AIs to specifically focus on:

- commitment of adequate resources with required knowledge and clear accountability for effective oversight of e-banking services outsourced to outside technology service providers;
- ensuring that the outsourced service is subject to independent assessment (see also subsection 2.4 and Annex A); and
- for cross-border outsourcing, ensuring that the arrangements meet the applicable laws, regulations and supervisory standards.

5. Customer security and other risk management controls

5.1 Consumer protection

5.1.1 As for other banking services for personal customers, AIs are required to observe the Code of Banking Practice in providing e-banking services to their personal customers.

5.1.2 AIs must set out clearly in their terms and conditions the respective rights and obligations between the institutions and their customers. These terms and conditions should be fair and balanced to both the institutions and the

customers. In line with the Code of Banking Practice, the HKMA's view is that unless a customer acts fraudulently or with gross negligence, he should not be responsible for any direct loss suffered by him as a result of unauthorized transactions conducted through his account.

5.2 Administration of e-banking accounts

5.2.1 If AIs allow their existing customers to open an e-banking account online, they should ensure that adequate controls are in place to minimise the risks of e-banking accounts being opened by fraudsters without the knowledge of the genuine customers.

5.2.2 A reliable authentication method[17] should be adopted to verify the identity of a person who opens an e-banking account online. In addition, AIs should issue written confirmation to the customer concerned. It would also be helpful if the e-banking account is prohibited from effecting online transfers to unregistered third parties until AIs are satisfied that the customer concerned has received the confirmation (see also subsection 5.3 below).

5.2.3 AIs should perform adequate identity checks when any customer requests a change to the customer's e-banking account information or other contact details that are useful for the customer to monitor the activities of his accounts. These include resetting or reissuing of the customer's e-banking password, and changing contact information such as e-mail address, correspondence

[17] If the authentication method involves customers inputting the PIN of their credit/ATM cards or phone-banking accounts and credit card/account number concerned, the AI should implement adequate controls over resetting or re-issuing of the PIN. In particular, the new PIN should be delivered to customers through secure channels such as the branch network or by post to the customers' registered addresses. Resetting of the PIN by inputting personal data over the telephone or other electronic channels should generally not be allowed unless stronger customer authentication such as multi-factor authentication is employed or more stringent control is in place, e.g. suspending the e-banking account until the AI has verified the customer's identity through another channel. AIs should also put in place procedures to reduce the risk that the related sensitive information can be obtained by fraudsters, say, through mail thefts. For example, AIs should ensure that the credit/ATM card is received properly by the customer before issuing the PIN. Where AIs send out written notices to customers for collection of their credit/ATM card in person, the notice should not contain the credit card/account number.

address or contact phone number. AIs should consider the following measures or any combination thereof when handling these requests:

- for change requests personally submitted by customers at branches, checking customers' signatures and, where necessary, their identity cards or passports;
- assessing the risk related to change requests (e.g. correspondence address change) received by post or drop-in boxes at branches and, where necessary, reconfirming with customers through appropriate channels (e.g. telephone) before effecting the changes;
- for change requests initiated through the e-banking services as well as other channels, ensuring that effective monitoring mechanisms are in place (see subsection 5.4 below);
- avoiding mailing important documents (e.g. new passwords, new cheque books and replacement of damaged credit cards) to a recently changed correspondence address particularly in the absence of measures similar to the above three measures. In these cases, the customer concerned should be required to collect these documents at branches upon verification of his identity card or passport; and
- performing additional authentication checks of the customer's identity in respect of telephone requests for mailing of new passwords or other important documents, e.g. asking for information that changes over time in addition to questions relating to general personal particulars. Examples include approximate account balances and recent transactions.

5.3 Controls over fund transfers

5.3.1 AIs that rely solely on user IDs and passwords for customer authentication of e-banking services should consider restricting third-party transfers only to

accounts[18] that have been pre-registered by their customers. AIs should ensure the effectiveness of the restriction by requiring customers to register third-party accounts through secure channels (such as in person or by mail) and ensuring adequate authentication of customers' registration requests (see also para. 5.2.3).

5.3.2 As an alternative, customers may be allowed to register third-party accounts online but the registration should be made effective only after a period when a written confirmation is expected to have reached the customer.

5.3.3 If AIs, after balancing the pros and cons, decide to allow transfers to unregistered third-party accounts[19], they should put in place suitable safeguards to manage the risk of unauthorized third-party transfers, such as the following:

- the default transaction limit for online transfers to unregistered third parties (including both local and overseas payees) should be set to zero when the e-banking user account is first activated;
- AIs should ensure that customers are able to increase the limit only through secure channels (e.g. at branches or by mail) with adequate identity checks (see also para. 5.2.3);
- appropriate disclosure about the risk associated with these transfers to the customers should be made;
- for existing customers whose default limits for unregistered third-party transfer are non-zero, AIs may consider lowering these limits if the accounts have been inactive as regards unregistered third-party transfers;
- maximum daily or transaction limits should be imposed on online transfers to unregistered third parties. These limits should be lower than those for transfers to registered third parties;

[18] AIs should also assess the risk of online transfers to merchants that do not require registration in advance and implement similar controls as appropriate.

[19] These may include bill payments to unregistered accounts of non-utility companies such as jewellery stores, securities trading, and third-party credit card accounts.

- AIs may consider employing a second factor authentication before the customers may effect online transfers to unregistered third parties (see para. 4.1.2 above); and
- AIs should ideally implement two-factor authentication for corporate or institutional e-banking services that allow transfers to unregistered third-party accounts.

5.4 Monitoring of unusual activities

5.4.1 AIs should put in place effective monitoring mechanisms to detect, in a timely manner, suspicious online transactions and unusual activities. In particular, the monitoring mechanism for personal e-banking services should be able to detect cases similar to the following:

- many online transfers are made to the same unregistered third-party account within a short period of time especially if the amount transferred is close to the maximum amount allowed or the value exceeds a certain amount; and
- change of a customer's correspondence address[20] shortly followed by activities which may indicate potential fraudulent activities such as opening of an e-banking account online, a request for important documents (e.g. cheque book, new e-banking password, credit card/ATM PIN) to be mailed to that address, increase of fund transfer limits, or a sudden increase of fund transfers made to unregistered third parties.

5.4.2 AIs' monitoring staff should be promptly alerted by their monitoring mechanism if suspicious online transfers and unusual activities are initiated. In these cases, AIs should, as soon as practicable, check with the account holders of these transactions or activities.

5.4.3 Consideration could also be given to notifying personal customers immediately through an alternative automated channel (such as messages sent to mobile phones or e-

[20] AIs may need to pay special attention to cases where the requests for change of contact information such as correspondence address, telephone numbers and e-mail address are received by post at around the same time.

mail accounts of customers) of online transfers made to unregistered third parties, online transfers exceeding certain amount limits, or detected unusual activities related to their accounts.

5.5 Preventive controls relating to fake e-mails or websites

5.5.1 AIs should manage the risk associated with fraudulent e-mails or websites which are designed[21] to trick their customers into revealing private details such as account numbers or e-banking passwords. To this end, an AI should consider taking the following measures:

- letting customers know that the AI or its agents/business partners will never ask for their sensitive account information (such as PIN numbers or passwords) by e-mail. They should be asked to contact the AI by phone if in doubt;
- educating e-banking customers the ways to ensure that they are communicating with the official website, e.g. by clicking the padlock or key icon at the bottom of their browsers to check the relevant details[22] of the digital certificate of the transactional e-banking site, or by accessing the AI's website through the web browsers' bookmarks having satisfied themselves that the site bookmarked is genuine. Customers should be asked not to access the AI's transactional e-banking website through hyperlinks embedded in e-mails unless they have verified the genuineness of the website such as the validity of the digital certificate of the website; and
- searching the internet regularly to see if there are third-party websites with domain names which

[21] Fake e-mails and websites (e.g. accessed through hyperlinks embedded in fake e-mails) can look genuine by using different techniques such as (i) grabbing the genuine graphics from an AI's website; (ii) redirecting customers to the real websites so that customers are communicating with the real AI concerned without knowing that their private details may be passing through the fake websites; and (iii) using domain names which are very similar to that of an AI, or which may be regarded as those of an AI.

[22] Normally, customers should be advised on how to check the issuer of the certificate, whether the certificate is issued to the AI concerned and whether the certificate is still valid.

could be mistaken for that of the AI or websites which have established hyperlinks to the AI's site. If the intent of these websites is doubtful, the AI should consider blocking (e.g. through the firewall or router) any network traffic relayed by these websites to the AI's website, disputing the use of those domain names and seeking the assistance of the Police or the HKMA. Moreover, the AI may consider taking the initiative to register as appropriate domain names that are similar to, or can be mistaken as, the official domain name of the AI.

5.6 Customer education

5.6.1 As the devices used by customers to access e-banking services are beyond AIs' controls, security risks are likely to be heightened when a customer does not know or understand the necessary security precautions relating to the use of e-banking services. AIs should therefore pay special attention to the provision of easy-to-understand and prominent advice to their customers on e-banking security precautions. In particular, the Code of Banking Practice requires AIs to warn their personal e-banking customers of the obligations to take reasonable security precautions.

5.6.2 Depending on the types of e-banking customers and the nature of the e-banking services offered, AIs' security precautionary advice for customers should normally cover, at a minimum, the following:

- selection and protection of e-banking passwords (and user IDs if customers are allowed to select them). For instance, AIs should advise customers not to select passwords incorporating such information as birthday, telephone number or recognisable part of the customer's name. Customers should also be advised to avoid using the same password for accessing other online services (e.g. for internet access);

- safeguards against social engineering techniques[23]. Customers should be reminded not to disclose their personal information (e.g. information on their identity card or passport, addresses, or bank accounts) to any persons failing to prove their identities or any doubtful websites. In particular, customers should be alerted that they should never disclose their passwords to anyone including the AI's staff or the Police;
- reminding their customers not to access e-banking services through public or shared computers (e.g. at cyber cafés or public libraries);
- precautions that protect customers from being confused or deceived by fraudulent e-mails or websites (see subsection 5.5 above); and
- advising their customers to ensure that their PCs are securely configured and that they are adequately protected from computer viruses and malicious programs, for example, by installing a personal firewall and regularly updating their anti-virus software.

5.6.3 AIs may also refer to the security tips suggested to consumers from time to time by the Hong Kong Association of Banks (www.hkab.org.hk). Moreover, AIs should regularly review their security advice to ensure that it remains adequate and appropriate as their technology environment and e-banking services change.

5.6.4 Since customers may find it difficult to take in lengthy and complex advice, AIs should devise effective methods and channels for communicating with them on security precautions. AIs may make use of multiple channels (e.g. AIs' websites, messages printed on customer statements, promotional leaflets, circumstances when AIs' frontline staff communicate with their customers) to reinforce certain key precautionary measures.

[23] Social engineering is a scheme using social techniques to attempt to gain information or access. For example, a perpetrator may claim to be someone from an AI to get the victim to reveal his personal information, user ID or password.

5.7 Legal and reputation risk management

5.7.1 AIs should perform appropriate assessment of the legal and reputation risks associated with their e-banking services. This assessment is particularly important when e-banking services are offered to, or potentially regarded as targeting at, another jurisdiction.

5.7.2 Based on the risk assessment, AIs should have in place proper controls to manage the legal and reputation risks. For example, the controls may include:

- proper terms and conditions of e-banking services;
- appropriate disclosure and disclaimer prominently posted on the e-banking websites or other relevant documents so as to address the applicable legal requirements (e.g. the Personal Data (Privacy) Ordinance, consumer protection regulations of overseas jurisdictions) and potential reputation issues; and
- consideration of the need to use appropriate insurance coverage to address residual legal risks.

5.7.3 In the event that an AI intends to introduce a new e-banking service (e.g. payment service) which is not available through existing delivery channels, the AI is expected to have regard to the same supervisory requirements and risk management principles as set out in this module, including the legal and reputation risk.

5.7.4 For instance, the account aggregation service[24] normally entails retrieval of relevant information (e.g. account balance) of a customer's online accounts maintained in other organisations. AIs should evaluate carefully the security, legal and reputation risks associated with this service before offering it to their customers. Depending

[24] An account aggregation service allows customers to view their online accounts maintained in different organisations on a single website with a single sign-on user ID and password. Certain overseas account aggregation services involve customers providing their user IDs and passwords of their online accounts to the aggregators for accessing and consolidaing customers' relavant information on the single website. Depending on the implementation of the service, there may be a need to address the issue related to the security protection of customers' passwords and confidential information.

on the mechanism of the retrieval process (particularly the roles played by the AI and the customer in retrieving the information), the legal and reputation implications for the service could be different and need to be appropriately assessed by the AI.

Annex A: Scope and reporting of independent assessment

A1. In general, the independent assessment should cover at least the following areas, taking into account the guidance in sections 3 to 5 of this module:

Board and senior management oversight

A1.1 To assess whether the senior management of the AI have approved and issued comprehensive information security policies relevant to the e-banking service, put in place an effective management structure to ensure that these are implemented, enforced and regularly maintained in the institution;

Customer authentication and information protection

A1.2 To assess whether appropriate techniques have been implemented to enable the AI to authenticate the identity and authority of customers using the e-banking service;

A1.3 To assess whether appropriate techniques have been implemented to protect the confidentiality and integrity of information while it is stored or in passage over external and internal networks;

Application security, internet infrastructure and security monitoring

A1.4 To assess whether adequate application security has been implemented in the e-banking systems, including: use of appropriate development tools that provide effective security features; proper design, review and protection of application code and file directories; and comprehensive validation of input parameters;

A1.5 To assess whether appropriate security measures[25] (including system design and configuration of the servers[26], firewalls and routers, and network security)

---

[25] The independent assessment should cover not only the security aspects of network connections between external public networks such as the internet and the AI's own servers or firewalls, but also the security aspects of the network connections and system interfaces between these servers/firewalls and the AI's internal systems and databases.

[26] It should be noted that proper security arrangements of certain services (e.g. e-mail services for communicating with e-banking customers, and domain name service (DNS) for translating website names into network addresses and vice versa) involving communications with public networks are also important in preventing attacks on the e-

have been implemented to provide reasonable assurance that the DMZ, e-banking systems, internal networks of the AI and the network connections to public networks or remote parties are protected;

A1.6 To assess whether appropriate measures have been implemented to detect and record unusual activities, intrusion, or weaknesses on an ongoing basis, including the maintenance and review of audit trails or transaction logs, and whether appropriate procedures have been put in place to report and response to such incidents;

A1.7 To assess whether appropriate physical security measures have been implemented to ensure that unauthorized physical access to critical computer or network equipment can be prevented;

A1.8 To assess whether appropriate change control policies and procedures for the related applications, system and network components have been put in place to ensure that all changes to the production systems and networks are properly approved, tested and implemented;

Incident response and business continuity management

A1.9 To assess whether adequate operational and performance monitoring procedures have been implemented and performance criteria have been specified to ensure that the performance monitoring statistics have been analysed on a timely basis and appropriate actions have been taken to address any related problems;

A1.10 To assess whether appropriate measures have been incorporated in the design of the e-banking system and internet infrastructure (e.g. redundancy of key system components) to provide reasonable assurance of preventing disruptions to the system, mitigating the impact of disruptions and/or responding to disruptions;

A1.11 To assess whether appropriate BCPs and procedures have been developed to deal with material disruptions to, and to resume, the AI's e-banking service;

---

banking systems through these services. As a result, the independent assessment should also cover the security aspects of relevant servers (e.g. DNS servers, mail servers) for such services.

A1.12 To assess whether appropriate arrangements have been put in place to maintain, validate and rehearse the BCP, at a minimum, on an annual basis;

Customer security

A1.13 To assess whether appropriate steps have been taken to provide prominent advice to customers on the security precautions they need to take in relation to the e-banking service;

A1.14 To assess the effectiveness of the control procedures for e-banking account administration, including account opening, issue or reset of passwords, registration of third party accounts, and change of account information; and

A1.15 To assess whether appropriate measures have been implemented for handling high risk transactions such as unregistered third party fund transfers and online payments.

A2. Content of an independent assessment report

Period of assessment

A2.1 The report should state when and at what stage of development of the system (e.g. design stage or testing stage) the independent assessment was conducted.

Scope & approach

A2.2 The report should describe the scope of, and approach adopted in, the assessment. In particular, the scope should clearly set out what system components, as well as what portion of the AI's internal networks and network equipment (e.g. gateways and routers) are covered in the independent assessment.

A2.3 The assessor should perform more thorough review on areas of higher risk. For AIs offering e-banking services of higher risk (e.g. services allowing large-value funds transfer to unregistered third-party accounts), they should consider including in their independent assessments penetration testing having regard to different types of online attacks.

Summary of assessment results

A2.4 The report should include the following information:

- findings identified in the assessment. These may also include explanation of the security implications of the findings, and the assessor's assessment of the level of risk associated with the findings;
- recommendations of the assessor to assist in addressing the findings; and
- management response to the findings and recommendations, including the actions to be taken to address the findings, the target date for completing the actions, and any interim measures to be taken (the management response may be included in a separate report).

A2.5 If the management adopt alternative methods to address the weaknesses identified by the assessor or if the assessment discloses material weaknesses, the AI may request the assessor or other independent expert to perform a follow-up review.

A3. Independent assessment of outsourced operations

A3.1 If an AI's e-banking service has been outsourced (partly or entirely) to an outside service provider, the senior management of the AI should ensure that the outside service provider commissions adequate independent assessments, provides the AI with the results of the assessments and regularly evaluates the adequacy of its security arrangements in between independent assessments.

A3.2 The selection of the assessor and, the frequency and the scope of the independent assessment commissioned by the outside service provider should be comparable with those suggested in subsection 2.4 and this annex, and have taken into account the latest technological developments and industry sound practices.

Annex B: Sound practices for the establishment of internet infrastructure

B1. Background

B1.1 This annex provides AIs with sound practices for the establishment of their internet infrastructure, including the design and configuration of servers in the DMZ, firewalls and routers, and the use of IDSs. It should be stressed that this annex is not intended to be exhaustive. AIs should also make reference to the industry sound practices[27] and put in place internet infrastructure which is commensurate with the risks associated with their e-banking services.

B2. Servers in DMZ

B2.1 The internet infrastructure or DMZ normally houses various kinds of servers, including the application servers, web servers, the DNS server and the mail server. Depending on the types of implementation, some servers may handle the front-end processing of the internet-based e-banking system, such as validation of data entered by customers or responding to customers. Given the exposure of these servers to attacks from any user via the internet, no confidential data should be stored in these servers.

B3. Firewalls and routers

B3.1 Firewalls and routers should be appropriately chosen, configured and installed. There should be "external firewall(s)" to control the traffic between the internet and the servers housed in the DMZ so that only acceptable communication methods for connecting to these servers would be allowed as attackers may exploit certain communication methods to pose threats to these

[27] AIs may find it useful to refer to other references on security of internet infrastructure (e.g. SANS (System Administration, Networking and Security) Institute (www.sans.org) and the Computer Emergency Response Team (www.cert.org).

servers[28]. No sensitive or system information should be unveiled when the firewalls respond to malicious network traffic from the internet.

B3.2 In ensuring that only the allowed types of traffic can pass through from the servers in the DMZ to the AIs' trusted internal networks, AIs should ideally install another tier of "internal firewall(s)" to control the traffic between the servers in the DMZ and the AIs' trusted internal networks. In addition, if two or more tiers of firewalls are used, AIs may consider using firewalls of different types to prevent similar security vulnerabilities from being exploited in different firewalls.

B3.3 The effectiveness of firewalls and routers as a security tool is heavily dependent upon how the firewalls or routers are configured and the policies in place in respect of their configuration and maintenance. It is important that AIs should formulate and document formal policies for the configuration, monitoring and maintenance of their firewalls and routers, so that all changes to the configuration are properly controlled, tested and tracked.

B3.4 AIs should perform frequent reviews and timely updates of the firewall and router configurations to enhance protection from newly identified vulnerabilities and system weaknesses. Given the complexity involved in this process, it is important for AIs to carefully select reputable vendors who are able to keep abreast of the latest improvements needed in the firewalls and routers to protect from the latest attack techniques.

B3.5 Any direct dial-up connections or other network connections with third parties bypassing the firewalls should be generally prohibited. If a dial-up connection is necessary for a specific task, this connection should be properly approved, monitored and removed immediately after completion of the task.

B3.6 Network traffic for firewall administration should be confined within a system administration segment of AIs'

[28] For example, “Telnet” is a communication method that allows remote users to sign on to a server (other than through browsers), thereby raising the risk of these users seizing control of the server.

internal networks, which is separated from the network segment connected to the production systems, so that the production network and systems would not be affected by the firewall administration activities.

B4. Additional security measures

B4.1 Any unused programs and computer processes of the servers, firewalls and routers should be deactivated or removed. AIs should establish accountability for the timely review, testing and application of appropriate patches to servers, firewalls and routers. Moreover, anti-virus software should be installed and updated on servers and firewalls as necessary. Only the minimum number of user accounts that are necessary for the operation of the routers, firewalls and servers should be maintained.

B4.2 The programs and other information kept in the servers, firewalls and routers should be updated only by strongly authenticated user accounts or authorized computer processes. They should also be subject to stringent change control procedures. AIs should use appropriate scanning tools to identify any potential security issues of the operating environment on a regular basis. Periodic integrity checks on the programs and static data (e.g. configuration) kept in servers and firewalls should be conducted to validate that they have not been altered.

B4.3 All access to the servers, firewalls and routers using privileged or emergency accounts (e.g. system administrator or "super user") should be tightly controlled, recorded and monitored (e.g. peer reviews). For example, logins from these accounts should be restricted only from physically secure terminals or, if servers, firewalls and routers are administrated remotely, strong authentication and encryption of system information should be in place to protect them from unauthorized access.

B4.4 Redundancies should be built into the critical components of the internet infrastructure to avoid any single points of failure which can bring down the entire network and infrastructure.

B5. Intrusion detection and use of IDSs

B5.1 AIs should identify cautiously the information necessary to detect an intrusion in the internet infrastructure. This information facilitates AIs to determine what audit logs of the servers, firewalls and routers should be enabled and, if necessary, what other data (e.g. system resources utilisation, network traffic) should be monitored.

B5.2 Appropriate controls should be in place to protect and backup the audit logs, and to ensure that the clocks of the systems generating the logs are synchronised. Audit logs should generally be reviewed on a daily basis. Since log files are typically voluminous and difficult for humans to process, AIs should consider the use of IDSs to analyse the audit logs and to collect other information that is relevant and not available from the audit logs.

B5.3 In selecting IDS products, AIs should consider whether the products can provide the information required for detecting potential intrusion and whether the vendors are able to offer timely updates of attack signatures (i.e. pre-defined patterns of activities for detection of possible intrusion).

B5.4 A host-based IDS can detect probable intrusion of a host (e.g. web server, firewall) by identifying unauthorized activities recorded in audit logs or alteration of its configuration or other important files. A network-based IDS can monitor and detect unusual traffic transmitting to and from the computers, and on the network segment.

B5.5 IDSs should be tested and their attack signatures and alert settings should be fine-tuned periodically to improve their effectiveness while reducing false alarms. A process should be in place to ensure that the relevant support staff should respond to important alerts generated by IDSs on a 24 hours by 7 days basis.