Independent Assessment of Security Aspects of Transactional E-banking Services

An HKMA Guidance Note

Purpose

To specify the expected scope of independent assessments of the security aspects of transactional e-banking services and to provide general guidance on selecting the assessors and on the types of information to be included in the independent assessment reports.

Classification

A guidance note issued by the HKMA.

Previous guidelines / guidance notes superseded

This is a new guidance note which supplements the circular entitled Electronic Banking of 7 July 1997 and the Guidance Note on Management of Security Risks in Electronic Banking Services of 6 July 2000.

Application

To all AIs

Structure

Independent Assessment of Security Aspects of Transactional E-banking Services

An HKMA Guidance Note

1. Introduction

1.1 As mentioned in the circular entitled Electronic Banking of 7 July 1997 and the Guidance Note on Management of Security Risks in Electronic Banking Services of 6 July 2000, given the paramount importance of managing the security risks of transactional e-banking services and the rapid pace of technological developments, the HKMA expects the senior management of AIs to commission periodic independent assessments of the security aspects of their transactional e-banking services.

1.2 The HKMA expects such independent assessments to be carried out by trusted independent experts (the "assessors") before the launch of the services, and generally thereafter at least once a year, or whenever there are substantial changes to the risk assessment of the services or major security breaches.

1.3 While AIs do not need to seek formal approval from the HKMA to introduce transactional e-banking services, AIs should discuss their plans with the HKMA in advance and submit the independent assessment reports for reference.

1.4 It is the responsibility of the senior management of each AI to manage the risks of its e-banking service. Consequently, it is the responsibility of the senior management to assess the risks attaching to their e-banking service and to determine the extent of review.

2. Proposed scope of independent assessment

2.1 The assessor is expected to evaluate the information security policies, internal controls and procedures, as well as system and network security, taking into account the expectations and recommendations in the HKMA circulars and guidance notes, the latest technological developments and security threats, and industry standards and sound practices.

2.2 Generally, the independent assessment should cover at least the following areas:

Information security policies and practices

2.2.1 To assess whether the senior management of the AI have issued and maintained comprehensive information security policies relevant to the e-banking service, put in place an effective management structure to ensure that

these are implemented and enforced, and encourage the development of a security culture in the institution;

2.2.2 To assess whether appropriate physical security measures have been implemented to provide reasonable assurance that unauthorized physical access to critical computer or network equipment can be prevented;

2.2.3 To assess whether appropriate security measures including comprehensive contractual agreements (e.g., service level agreement, consultancy agreement, confidentiality agreement) have been put in place in relation to the security risks arising from business counterparties and other external parties;

2.2.4 To assess whether appropriate steps have been taken to provide easy-to-understand and prominent advice to customers on the security precautions they need to take in relation to the e-banking service;

2.2.5 To assess whether the senior management of the AI have put in place a mechanism for commissioning periodic evaluations of the continued effectiveness of the information security policies and practices, as well as the system and network security relating to the e-banking service;

2.2.6 To assess whether appropriate measures have been implemented to detect and record intrusion, security breaches or weaknesses on an ongoing basis, including the maintenance of audit trails or transaction logs, and whether appropriate procedures have been put in place to report and handle such incidents;

2.2.7 To assess whether appropriate change control policies and procedures for the related applications, system and network components have been put in place to provide a reasonable assurance that all changes to the production systems and networks are properly tested, approved and recorded;

System and network security

2.2.8 To assess whether appropriate security measures[1] have been implemented to provide reasonable assurance that the internal networks of the AI and the network connections to public networks or remote parties are protected;

2.2.9 To assess whether appropriate security measures have been implemented such as in the system design and configuration of the servers[2] and firewalls that support and protect the e-banking service (particularly internet-based transactional e-banking service);

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

2.2.11 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, and to enable customers to validate the genuineness of the system accessed by them.

2.2.12 To assess whether appropriate techniques have been implemented to ensure the integrity of information transmitted over networks.

Business continuity management

2.2.13 To assess whether appropriate measures have been incorporated in the design of the e-banking system (e.g., redundancy of key system components, specific configuration of firewalls) to provide reasonable

---

[1] 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.

[2] It should be noted that proper security arrangements of certain services (e.g., e-mail services for communicating with e-banking customers, Domain Name System (DNS) for translating web site names into network addresses) involving communications with public networks are also important in preventing attacks on the e-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.

assurance of preventing disruptions to the system, mitigating the impact of disruptions and/or responding to disruptions. This should have regard to the AI's assessment of the risk and impact of any disruptions (including interruptions due to malicious attacks);

2.2.14 To assess whether appropriate business continuity plans and procedures have been developed to deal with material disruptions to the AI's e-banking service. For instance, these may cover the following areas:

- arrangements to handle disruptions to the production environment (e.g., electricity failures, production site difficulties), failure of service providers (e.g., outsourcing operators, telecommunication operators) and loss of data;
- plans and procedures for dealing with interruptions caused by attacks such as Denial of Services (DoS) and Distributed Denial of Services (DDoS);
- procedures for providing alternative channels for delivering services and the related customer support issues, including emergency staffing arrangements;
- public relations and communication strategy for safeguarding the AI's reputation.

2.2.15 To assess whether appropriate arrangements have been put in place to maintain, validate and rehearse the business continuity plans and procedures (including any data back-up procedures) on an ongoing basis.

3. Previous independent assessments

3.1 In the event that an AI has previously conducted independent assessments of certain aspects of its e-banking service, it may take these previous assessments into account in deciding the scope of assessment of other e-banking services. For instance, an AI which introduces e-banking services by phases may have already had an independent assessment of certain aspects (e.g., firewalls and routers) relevant to all phases. In this case, there may not be a need for the AI to cover those aspects in subsequent independent assessments.

3.2 However, if the previous assessments were conducted a long time before or there are recent security breaches or threats relating to the controls reviewed in previous assessments, the AI should consider whether an updated assessment is necessary.

4. Selection of the assessor

4.1 The assessor should have the necessary expertise in the field to perform the independent assessment. In general, the HKMA expects that the assessor should be an external party (e.g., an external auditor or third-party security consultant). However, in some cases, it may also be acceptable for an AI's internal staff (e.g., internal auditors) or an independent unit of the vendor of the relevant e-banking system to conduct the independent assessment provided that they can demonstrate that they have the necessary expertise to carry out such assessments. However, they should be independent from the parties that develop, implement or operate the services.

4.2 To ensure impartiality, the assessor should not be involved in the operations to be reviewed or in selecting or implementing the relevant control measures to be reviewed (although the assessor may have commented on some aspects of the control measures or the e-banking system in the past). The assessor should be able to report its findings freely and directly to the senior management of the AI as appropriate.

4.3 The HKMA should be notified of the party to be appointed as the assessor. If necessary, the HKMA may request further information from the relevant AI about the assessor.

5. Independent assessment by multiple assessors

5.1 An AI may decide to engage different parties (e.g., internal auditors, external auditors or security consultants) to conduct independent assessment of different aspects of its e-banking system. If this is the case, the AI should specify the scope of assessment to be performed by each party. It should ensure that there are no material gaps among different assessments and, taken as a whole, the assessments should enable senior management to form an overall view of the security of the e-banking service.

6. Proposed content of an independent assessment report

6.1 Period of assessment

6.1.1 The report should state when and at what stage of introduction of the service (e.g., design stage, testing stage) the independent assessment was conducted.

6.1.2 In general, independent assessment should be largely completed and the report submitted to the senior management of the AI and forwarded to the HKMA for reference before the launch of new e-banking services, except for those reviews (e.g., follow-up on non-critical issues, reviews of production operations of e-banking service) that cannot be reasonably completed before the launch of the services.

6.2 Scope & approach

6.2.1 The report should describe the scope of, and approach adopted in, the assessment. In particular, the scope should clearly set out what servers (e.g., web server, application server, database server, mail server, DNS server) and firewalls, as well as what portion of the AI's internal networks and network equipment (e.g., gateways, routers) are covered in the independent assessment. If the scope of assessment is materially different from the proposed scope as mentioned in section 2 above, an explanation of the differences should be provided.

6.2.2 As regards the approach adopted by the assessor, the assessor may take into account discussions with relevant personnel of the institution, supported by review of documentary evidence as appropriate. The assessor may also take steps to validate the information provided by the AI, such as through physical inspection or the use of scanning tools[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 high-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.

6.3 Basis of assessment

6.3.1 The report should describe the basis of assessment. While the HKMA does not prescribe e-banking security

[3] Scanning tools are commercially available tools that can be used for identifying and analysing security vulnerabilities in networks, operating systems and databases.

standards, it is important that the assessor has considered the relevant HKMA circulars and guidance notes, industry standards or sound practices, and the latest technological developments and security threats in forming the basis of assessment.

6.3.2 As it is possible that some of the controls may not be in place or tested at the time of assessment, the report should indicate where the assessment is based on the review of controls that are in place and the review of "planned" controls respectively.

6.4 Summary of assessment results

6.4.1 The report should include the following information:

- Findings identified in the assessment, 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;

- 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. If the management do not entirely agree with the findings or recommendations, or decide to deploy alternative methods to address the findings, an explanation should be provided;

- 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 to perform a follow-up review.

7. Independent assessment of outsourced operations

7.1 If an AI's e-banking service has been outsourced (partly or entirely) to an outsourcing operator, the senior management of the AI should ensure that the outsourcing operator commissions adequate independent assessments, provides the AI with the results of the assessments (which will then be provided to the HKMA) and regularly evaluates the adequacy of its security arrangements in between independent assessments.

7.2 In particular, the senior management of the AI should ensure that:

7.2.1 the assessor commissioned by the outsourcing operator to conduct independent assessment of the security aspects of the outsourced e-banking service has adequate independence and expertise (e.g., principles similar to those for the AI's own independent assessment should be followed);

7.2.2 the scope and basis of the independent assessment commissioned by the outsourcing operator are comparable with those suggested in this Guidance Note, and have taken into account the relevant HKMA circulars and guidance notes, the latest technological developments and security threats, and industry standards and sound practices;

7.2.3 the assessor has adopted an appropriate approach (e.g., combination of interview and review of documentary evidence or design and configuration of the system as appropriate) to conduct the independent assessment;

7.2.4 findings identified in the independent assessment are properly addressed by the outsourcing operator.

7.3 The senior management of the AI should liaise with the outsourcing operator to determine whether further independent assessment should be commissioned, having regard to factors such as:

7.3.1 any inadequacy or concerns regarding the independent assessment engaged by the outsourcing operator (e.g., as regards the expertise or independence of the assessor commissioned by the outsourcing operator, or approach adopted by the assessor, etc);

7.3.2 any other issues that are not covered by the outsourcing operator's independent assessment (e.g., system interfaces between the systems of the AI and those of the outsourcing operator).

Independent Assessment of Security Aspects of Transactional E-banking Services

An HKMA Guidance Note

Hong Kong Monetary Authority