

# IS AUDITING GUIDELINE

## INTERNET BANKING

DOCUMENT G24

**Introduction**—The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association® (ISACA®) is to advance globally applicable standards to meet this need. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community.

**Objectives**—The objectives of the ISACA IS Auditing Standards are to inform:

- IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the *ISACA Code of Professional Ethics* for IS auditors
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
- The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

**Scope and Authority of IS Auditing Standards**—The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting.
- **Guidelines** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. Procedures should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtain the same results. In determining the appropriateness of any specific procedure, group of procedures or test, IS auditors should apply their own professional judgment to the specific circumstances presented by the particular information systems or technology environment. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

The words audit and review are used interchangeably. A full glossary of terms can be found on the ISACA web site at [www.isaca.org/glossary.htm](http://www.isaca.org/glossary.htm).

Holders of the Certified Information Systems Auditor™ (CISA®) designation are to comply with IS Auditing Standards adopted by ISACA. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

**Development of Standards, Guidelines and Procedures**—The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation, where necessary.

The following COBIT® resources should be used as a source of best practice guidance:

- *Control Objectives*—High-level and detailed generic statements of minimum good control
- *Control Practices*—Practical rationales and how-to-implement guidance for the control objectives
- *Audit Guidelines*—Guidance for each control area on how to: obtain an understanding, evaluate each control, assess compliance, and substantiate the risk of controls not being met
- *Management Guidelines*—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors

Each of these is organised by the IT management process, as defined in the *COBIT Framework*. COBIT is intended for use by businesses and IT management as well as IS auditors. Its usage allows for the understanding of business objectives and for the communication of best practices and recommendations around a commonly understood and well-respected standard reference.

The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to help identify emerging issues requiring new standards. Any suggestions should be e-mailed ([research@isaca.org](mailto:research@isaca.org)), faxed (+1.847.253.1443) or mailed (address at the end of this guideline) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This material was issued on 1 May 2003.

### Information Systems Audit and Control Association 2002-2003 Standards Board

Chair, Claudio Cilli, CISA, CISM, CIA, Ph.D., CISSP KPMG, Italy  
Claude Carter, CISA, CA Nova Scotia Auditor General's Office, Canada  
Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay  
Alonso Hernandez, CISA, ROAC Colegio Economistas, Spain  
Marcelo Hector Gonzalez, CISA Central Bank of Argentina Republic, Argentina  
Andrew MacLeod, CISA, FCPA, MACS, PCP, CIA Brisbane City Council, Australia  
Peter Niblett, CISA, CA, MIIA, FCPA Day Neilson, Australia  
John G. Ott, CISA, CPA Aetna, Inc., USA  
Venkatakrishnan Vatsaraman, CISA, ACA, AICWA, CISSP Emirates Airlines, United Arab Emirates

## **1. BACKGROUND**

### **1.1 Linkage to ISACA Standards**

- 1.1.1** Standard S2 Independence states, "The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment."
- 1.1.2** Standard S4 Professional Competence states, "The IS auditor should be technically competent, having the skills and knowledge to conduct the audit assignment."
- 1.1.3** Standard S5 Planning states, "The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards."
- 1.1.4** Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."
- 1.1.5** Guideline G22 Business to Consumer E-commerce Reviews provides guidance.
- 1.1.6** Procedure P3 Intrusion Detection System Review provides guidance.
- 1.1.7** Procedure P2 Digital Signatures and Key Management provides guidance.

### **1.2 Linkage to COBIT**

- 1.2.1** The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."
- 1.2.2** The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
  - Performance measurement—How well is the IT function supporting business requirements?
  - IT control profiling—What IT processes are important? What are the critical success factors for control?
  - Awareness—What are the risks of not achieving the objectives?
  - Benchmarking—What do others do? How can results be measured and compared?
- 1.2.3** The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.
- 1.2.4** The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
- 1.2.5** COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.
- 1.2.6** Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

### **1.3 Need for Guideline**

- 1.3.1** The purpose of this guideline is to describe the recommended practices to carry out the review of Internet banking initiatives, applications and implementations, as well as to help identify and control the risks associated with this activity, so that the relevant IS Auditing Standards are complied with during the course of the review.

## **2. INTERNET BANKING**

### **2.1 Definition**

- 2.1.1** The term Internet banking refers to the use of the Internet as a remote delivery channel for banking services. Services include the traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic online payments (allowing customers to receive and pay bills on a bank's web site).

### **2.2 Internet Banking Activities**

- 2.2.1** More and more banks are transforming their businesses by using Internet technology to develop or expand relationships with their customers. The extent to which the Internet is used in a bank depends on the relative maturity of the bank in regard to Internet technology. Banks offer Internet banking in two main ways. An existing bank with physical offices, ordinarily termed a brick-and-mortar bank, can establish a web site and offer Internet banking to its customers as an addition to its traditional delivery channels. An alternative is to establish either a virtual, branchless or Internet-only bank. The computer server or bank database that lies at the heart of a virtual bank may be housed in an office that serves as the legal address of such a bank or at some other location. Virtual banks provide customers with the ability to make deposits and withdrawals via automated teller machines (ATMs) or through other remote delivery channels owned by other institutions. Characteristics of Internet banking include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of the Internet, the integration of Internet banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology. Accordingly, a bank can perform Internet activities in one or more of the following ways:
  - Informational—This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. Risks associated with these operations are relatively low, as informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or can be outsourced. While the risk to a bank is relatively low, the data on the server or web site may

be vulnerable to alteration. Appropriate controls, therefore, must be in place to prevent unauthorised alterations of the data on the bank's server or web site.

- **Communicative**—This type of Internet banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications or static file updates (name and address changes). Because these servers ordinarily have a direct path to the bank's internal networks, the operational risk is higher with this configuration than with informational systems. Controls should be in place to prevent, monitor and alert management of any unauthorised attempt to access the bank's internal networks and computer systems. Virus detection and prevention controls are also important in this environment.
- **Transactional**—This level of Internet banking allows customers to directly execute transactions with financial implications. There are two levels of transactional Internet banking, each with a different risk profile. The basic transactional site only allows a transfer of funds between the accounts of one customer and the bank. The advanced transactional site provides a means for generating payments directly to third parties outside of the bank. This can take the form of bill payments via a bank official check or electronic funds transfer/automated clearing house entries. Many banks are also offering payments from consumer to consumer using either payment method. When the transfers of funds are allowed to a point outside of the bank, the operational risk increases. Unauthorised access in this environment can lead or give rise to fraud. Since a communication path is typically complex and may include passing through several public servers, lines or devices between the customer's and the bank's internal networks, this is the highest risk architecture and must have the strongest controls.

### **3. REVIEW OF INTERNET BANKING**

#### **3.1 Scope**

**3.1.1** Banking, by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputational, operational (including security—sometimes called transactional—and legal risks), credit, price, foreign exchange, interest rate and liquidity. Internet banking activities do not raise risks that were not already identified in traditional banking, but it increases and modifies some of these traditional risks. The core business and the information technology environment are tightly coupled, thereby influencing the overall risk profile of Internet banking. In particular, from the perspective of the IS auditor, the main issues are strategic, operational and reputational risk, as these are directly related to threats to reliable data flow and are heightened by the rapid introduction and underlying technological complexity of Internet banking. Banks should have a risk management process to enable them to identify, measure, monitor and control their technology risk exposure. Risk management of new technologies has three essential elements:

- Risk management is the responsibility of the board of directors and senior management. They are responsible for developing the bank's business strategy and establishing an effective risk management methodology. They need to possess the knowledge and skills to manage the bank's use of Internet banking and all related risks. The board should make an explicit, informed and documented strategic decision as to whether and how the bank is to provide Internet banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. The board should review, approve and monitor Internet banking technology-related projects that have a significant effect on the bank's risk profile and ensure that adequate controls are identified, planned and implemented.
- Implementing technology is the responsibility of information technology senior management. They should have the skills to effectively evaluate Internet banking technologies and products, and to ensure that they are installed and documented appropriately. If the bank does not have the expertise to fulfil this responsibility internally, it should consider contracting with a vendor who specialises in this type of business or engaging in an alliance with another third party with complementary technologies or expertise.
- Measuring and monitoring risk is the responsibility of operational management. They should have the skills to effectively identify, measure, monitor and control risks associated with Internet banking. The board of directors should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed.

**3.1.2** Internal controls over Internet banking systems should be commensurate with the level of risk of the services the bank offers, the level of risk involved in the implementation and the bank's risk tolerance level. The review of internal control in the Internet banking environment must help the IS auditor to provide reasonable assurance that the controls are appropriate and function appropriately. Control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including effectiveness, efficiency and economy of operations and compliance with corporate policies and legal requirements
- Data and service availability, including business recovery planning
- Data integrity, including providing for safeguarding of assets, proper authorisation of transactions and reliability of the data flow
- Data confidentiality and privacy standards, including controls over access by both employees and customers
- Reliability of management reporting

**3.1.3** To appropriately evaluate the internal controls and their adequacy, the IS auditor should understand the bank's operational environment. COBIT 3<sup>rd</sup> Edition, published by the IT Governance Institute in 2000, has laid down seven information criteria to be met by information systems:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

**3.1.4** The information criteria listed in section 3.1.3 of this document are relevant in the case of Internet banking. Accordingly, a review

of Internet banking should address how the information criteria of COBIT are met by the Internet banking initiative/application/ implementation.

- 3.1.5** Compared with other forms/channels of banking activities, Internet banking depends greatly on the integrity or trust in the confidentiality of customer data and on the availability of the system. In this context, there should be in place appropriate redundancy and fallback options, as well as disaster recovery procedures. In the case of Internet banking involving payments or funds transfers, nonrepudiation and integrity of the transactions are essential attributes. In such cases, the review of Internet banking should address the effectiveness of the Internet banking system controls in assuring nonrepudiation and integrity. Due attention should be given to them while evaluating the availability of Internet banking solutions, especially if the continuity is based on cross-border processing, because it might infringe a regulation or might run counter to compliance with bank regulations.
- 3.1.6** It is essential in Internet banking to confirm that any communication, transaction or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions. Customer verification during account origination is important to reduce the risk of theft, fraudulent transactions and money laundering activities. Strong customer identification and authentication processes are particularly important in the cross-border context given the difficulties that may arise from doing business electronically with customers across national and international borders, including the risk of identity impersonation and the difficulty in conducting effective credit checks on potential customers.
- 3.1.7** Auditability has more significance in the Internet banking environment, because a significant proportion of the transactions take place in paperless environments.

## **4. INDEPENDENCE**

### **4.1 Professional Objectivity**

- 4.1.1** Before accepting the engagement, the IS auditor should provide reasonable assurance that any interests he/she may have in the Internet bank under review would not in any manner impair the objectivity of the review. In the event of any possible conflicts of interest, these should be explicitly communicated to the bank's management and the written approval of the bank's management should be obtained before accepting the assignment.

## **5. COMPETENCE**

### **5.1 Skills and Knowledge**

- 5.1.1** The IS auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking. The IS auditor should determine whether the technology and products are aligned with the bank's strategic goals. In particular, such reviews would call for bank operations knowledge and associated risks, knowledge of banking laws and regulations together with the technical knowledge necessary to evaluate aspects such as web hosting/web housing technologies, encryption technologies, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. Where expert advice or expert input is necessary, appropriate use should be made of external professional resources. The fact that external expert resources may be used should be communicated to the bank's management in writing.

## **6. PLANNING**

### **6.1 High-level Risk Assessment**

- 6.1.1** The IS auditor should gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives, the way that the bank is using Internet technology in the relationships with its customers (either informative, communicative or transactional, as set out in 2.2.1). The information thus gathered should be such that it helps in carrying out a high-level assessment of the banking risks as well as the risks pertaining to the information criteria of COBIT. This high-level risk assessment will help determine the scope and coverage of the review. If the bank has an enterprise risk framework, this can be used.
- 6.1.2** The IS auditor should follow a risk assessment approach for analysing and evaluating the main potential general and specific threats connected to implementation of Internet banking, the possible manifestations, the potential effect on the bank, the likelihood of occurrences and the possible risk management measures that can be implemented for preventing risks. The following strategic risks should be evaluated:
- The strategic assessment and risk analysis
  - Integration within corporate strategic goals
  - Selection and management of technological infrastructure
  - Comprehensive process for managing outsourcing relationships with third-party providers
- 6.1.3** The following security risks should be evaluated:
- Customer security practices
  - Authentication of customers
  - Nonrepudiation and accountability of transactions
  - Segregation of duties
  - Authorisation controls within systems, databases and applications
  - Internal or external fraud
  - Data integrity of transactions, databases and records
  - Audit trails for transactions
  - Confidentiality of data during transmission

- Third-party security risk

**6.1.4** The following legal risks should be evaluated:

- Disclosures of information to customers
- Privacy
- Compliance to laws, rules and statements of the regulator or supervisor
- Exposure to foreign jurisdictions

**6.1.5** The following reputational risks should be evaluated:

- Service level delivery
- Level of customer care
- Business continuity and contingency planning

## **6.2 Scope and Objectives of the Review**

**6.2.1** The IS auditor should, in consultation with the bank management where appropriate, clearly define the scope and objective of the review of Internet banking. The aspects to be covered by the review should be explicitly stated as part of the scope. The nature of the bank's Internet activities and volume of the Internet banking activities (set out in 2.2.1) and the risks associated with them—as identified by the high-level risk assessment—dictate which aspects need to be reviewed as well as the extent and depth of the review.

**6.2.2** For the purpose of the review, control objectives should be in accordance with regulations and applicable banking laws. The Internet is borderless, so it is easy for any bank using an Internet-based delivery channel to operate in a multi-state and even multi-country environment. The bank may find itself bound by the laws, regulations and customs of wherever its customers are located rather than just where the bank is physically located. Therefore, the IS auditor should determine the geographic spread of the bank's current and planned customer base. The IS auditor needs to identify how many different jurisdictions have legal and regulatory control over the Internet banking operations and determine how the Internet bank is managing this risk.

## **6.3 Approach**

**6.3.1** The IS auditor should formulate the approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre-implementation review or a post-implementation review. The approach should be appropriately documented. If the input or advice of external experts is to be used, this should also be specified as part of the approach.

## **6.4 Sign-off for the Plan**

**6.4.1** Depending on the practices of the organisation, it may be appropriate for the IS auditor to obtain the agreement of the bank's management for the review plan and approach.

# **7. PERFORMANCE OF INTERNET BANKING REVIEW**

## **7.1 Execution**

**7.1.1** The aspects to be reviewed and the review process should be chosen by taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.

**7.1.2** In general, in gathering, analysing and interpreting the Internet banking environment, a study should be made of available documentation, such as bank regulations about Internet banking, Internet law, privacy law, web banking system documentation and use of the Internet banking solution.

**7.1.3** To identify any problems relating to the Internet banking area which have been noted previously and which may require follow-up, the IS auditor should review the following documents:

- Previous examination reports
- Follow-up activities
- Work papers from previous examinations
- Internal and external audit reports

**7.1.4** The IS auditor should map the key processes—both automated as well as manual—relating to the Internet banking initiative/system.

**7.1.5** The assessment of the core business risks (set out in 6.1) should include a critical evaluation of the Internet banking objectives, strategy and business model.

**7.1.6** The IS auditor should then assess the probability that the risks identified pertaining to these processes (business as well as IS risks) will materialise together with their likely effect, and document the risks along with the controls, which mitigate these risks.

**7.1.7** As part of the IS risk assessment, external IS threats should be evaluated depending on the nature of products offered by a bank and the external threats to be addressed. These threats include denial of service, unauthorised access to data, unauthorised use of the computer equipment, which could arise from various sources such as casual hackers, competitors, alien governments, terrorists or disgruntled employees.

**7.1.8** Depending on the nature of the pre- or post-implementation review, the IS auditor should test the significant processes in the test and or production environment to verify that the processes are functioning as intended. These tests include testing of balance inquiry, testing of bill presentation and payment and testing the security mechanisms using penetration testing.

**7.1.9** In post implementation review the IS auditor should obtain, at least, an understanding of network mapping, network routing, systems and network security assessment, and internal and external intrusion.

**7.1.10** Since the Internet banking solution is predominantly an information technology solution, it should meet the information criteria

established in COBIT, as well as other relevant standards or regulations of the industry. The extent of compliance with the information criteria, standards and/or regulations and the effect of noncompliance should be analysed.

## **7.2 Aspects to Review**

**7.2.1** The following organisational aspects should be reviewed for whether:

- Due diligence and risk analysis are performed before the bank conducts Internet banking activities
- Due diligence and risk analysis are performed where cross-border activities are conducted
- Internet banking is consistent with the bank's overall mission, strategic goals and operating plans
- Internet application is compliant with the defined and approved business model
- Internet banking systems and/or services are managed in-house or outsourced to a third-party
- Management and personnel of the organisation display acceptable knowledge and technical skills to manage Internet banking
- Measures to ensure segregation of duties are in place
- Management reports are adequate to appropriately manage Internet banking transaction and payment services activities

**7.2.2** The review should include policy aspects such as whether:

- Suitable policies have been defined and implemented regarding the acquisition of customers, the engagement of suppliers, the customers authentication, the privacy of customers/suppliers data, audit trail, the review of usage logs and whether the bank is keeping abreast of legal developments associated with Internet banking
- The bank is providing accurate privacy disclosures associated with its Internet banking product line
- Information is provided on the web site to allow customers to make informed judgment about the identity and regulatory status of the bank before they enter into Internet banking services (name of the bank and the location of its head office, the primary bank supervisory authority, ways to contact to customer service and other relevant information)
- The bank has established policies governing the use of hypertext links such that consumers can clearly distinguish between bank and non-bank products, and that they are informed when leaving the bank's web site
- There are appropriate procedures in place regarding change control, the review of audit trails and the review/analysis of usage logs (firewall logs and other reports)
- There are suitable and adequate procedures in place to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations as well as best practice

**7.2.3** The following planning aspects should be reviewed for whether:

- The planned information systems technology architecture is feasible and will result in safe and sound operations
- There are appropriate incident response plans in place to manage, contain and minimise problems arising from unexpected events, including internal or external attacks
- An "Internet product life cycle" exists and if it is followed both for developing, maintenance and upgrading Internet applications
- Business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested

**7.2.4** The following information systems infrastructure aspects should be reviewed for whether:

- The infrastructure and systems are capable of expansion to accommodate the proposed business plan
- An information security architecture has been defined and is appropriate for the nature of the Internet banking model
- The bank has an adequate process and controls to address physical security for hardware, software and data communications equipment associated with the Internet banking system
- The bank has a sound process which ensures adequate control over the path between the web site and the bank's internal networks or computer systems and whether the internal network is suitably protected from the external environment using appropriate firewall technology
- Databases and data flow are protected from unauthorised/inappropriate access
- There are suitable and adequate procedures in place to ensure the identification of access points and potential areas of vulnerability
- There are appropriate manual balancing controls where automated controls are inadequate
- The record for each customer transaction contains identification of the customer, the transaction number, the type of transaction, the transaction amount and other information of relevance, if it is stored and archived, for control purposes or other business functions such as marketing

**7.2.5** The following telecommunication infrastructure aspects should be reviewed for whether:

- The network architecture is appropriate for the nature, timing and extent of the Internet banking operation
- The network protocols used are appropriate for the intended use (for instance, if payments or funds transfers are accepted through the Internet banking system, secure protocols should be used)
- The bank has an effective process to assess the adequacy of physical controls in place to restrict access to firewall servers and components
- Intrusion detection systems and virus control systems/procedures are in place
- There is adequate penetration testing of internal or external networks
- The communication across the network is made secure using virtual private network (VPN) and related encryption techniques where appropriate and necessary
- Adequate and strong encryption algorithms were selected to protect data during communication across the network

**7.2.6** The following authentication aspects should be reviewed for whether:

- Control features are in place to validate the identity of prospective customers while they use the Internet to apply for new

- bank loan and/or deposit accounts
- Control features are built into the systems to ensure the authentication of the existing customer, the integrity of data and the confidentiality of transactions
- Authentication procedures are used to uniquely and positively identify the transacting party using digital certificates and digital signatures where necessary
- Nonrepudiation is ensured for an eventual later business or legal use where transactions are made using the Internet banking system
- The fault tolerance features of the Internet banking system are commensurate with the nature, volume and criticality of its system

**7.2.7** The following third-party service provider aspects should be reviewed for whether:

- Due diligence review of the competency and financial viability was conducted prior to entering into any contract with third-party service providers
- The contracts with third-party service providers adequately protect the interests of the bank and the bank's customers, and whether all outsourced systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards
- The bank organisation obtains and reviews internal or external audit reports of third-party service providers, evaluating vendor management processes or specific vendor relationships as they relate to information systems and technology, and whether all outsourced systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards
- The bank organisation has the right to conduct independent reviews and/or audits of security, internal control and business continuity and contingency plans of third-party service providers
- The security procedures of the third parties are appropriate and adequate where the Internet banking solution depends on the any third-party service providers such as Internet service providers (ISP), certification authority (CA), registration authority (RA), web-hosting/housing agency
- Third-party service providers have appropriate business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested, and whether the bank receives copies of test result reports
- The bank has an adequate process to ensure that software maintained by the vendor is under a software escrow agreement and that the software is confirmed as being current on a regular basis where the bank obtains software products from a vendor
- A third –party's opinion is sought in the pre-implementation phase of Internet applications for evaluating the security architecture solution that will be developed and configured

**7.2.8** Where necessary and agreed with the bank, external expert input or advice should be used suitably in the collection, analysis and interpretation of the data.

**7.2.9** The inferences and recommendations should be based on an objective analysis and interpretation of the data.

**7.2.10** Appropriate audit trails should be maintained and protected for the data gathered, the analysis made and the inferences arrived at, as well as the corrective actions recommended.

**7.2.11** Before finalising the report, the observations and recommendations should be validated with the stakeholders, board of directors and the bank's management, as appropriate.

## **8. REPORTING**

### **8.1 Report Content**

**8.1.2** The IS auditor should produce regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. Depending on the scope of its coverage, the report on Internet banking review carried out should address the following, as appropriate:

- The scope, objectives and methodology followed and assumptions
- An overall assessment of the Internet banking processes/systems solution in terms of key strengths and weaknesses as well as the likely effects of weaknesses
- Recommendations to overcome the significant weaknesses and to improve the Internet banking processes/systems solution
- A statement on the extent of compliance with bank regulations or applicable laws, along with the effect of any noncompliance
- A statement on the extent of compliance with the information criteria of COBIT, along with the effect of any noncompliance
- Recommendations regarding how the lessons of the review could be used to improve similar future solutions or initiatives

## **9. EFFECTIVE DATE**

**9.1** This guideline is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at [www.isaca.org/glossary.htm](http://www.isaca.org/glossary.htm).

## **APPENDIX**

### **COBIT Reference**

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

In the case of this specific audit area, Review of Internet Banking, the processes in COBIT likely to be the most relevant are: selected *Planning and Organising* IT processes, selected *Acquire and Implement* IT processes, selected *Delivery and Support*, and selected *Monitoring*. Therefore, COBIT guidance for the following processes should be considered relevant when performing the audit:

- PO1—Define a Strategic IT Plan
- PO3—Determine Technological Direction
- PO8—Ensure Compliance with External Requirements
- PO9—Assess Risk
- AI2—Acquire and maintain application software
- AI3—Acquire and maintain technology infrastructure
- AI4—Develop and maintain procedures
- AI5—Install and accredit systems
- AI6—Manage Changes
- DS1—Define and Manage Service Levels
- DS2—Manage Third-party Services
- DS3—Manage performance and capacity
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security
- DS8—Assist and Advise Customers
- DS10—Manage Problems and Incidents
- DS11—Manage Data
- M1—Monitoring the Process
- M2—Assess Internal Control Adequacy

The information criteria most relevant to an Internet Banking audit are:

- Primary: confidentiality, integrity, availability, compliance and reliability
- Secondary: effectiveness and efficiency

## References

- An Internet Banking Primer*, Federal Reserve Bank of Chicago, USA
- Basle Directive N° 82, Risk Management Principles for Electronic Banking*, Basel Committee on Banking Supervision, May 2001, Switzerland
- Basle Directive N° 86, Sound Practices for the Management and Supervision of Operational Risk*, Basel Committee on Banking Supervision, May 2001, Switzerland
- Basle Directive N° 91, Risk Management Principles for Electronic Banking*, Basel Committee on Banking Supervision, July 2002, Switzerland
- BIS Papers N° 7. Electronic finance: a new perspective and challenges*, Monetary and Economic Department, Bank for International Settlements, November 2001, Switzerland
- Cronin, Mary J., *Banking and Finance on the Internet*, John Wiley & Sons, Inc., ISBN 0-471-29219-2, USA
- Essinger, James, *The Virtual Banking Revolution*, Thomson Business Press, ISBN 1-86152-343-2, United Kingdom
- Internet Banking Comptroller's Handbook*, Comptroller of the Currency Administrator of National Banks, October 1999, USA
- Furst, Karen, William W. Lang and Daniel E. Nolle, *Internet Banking: Developments and Prospects*, Economic and Policy Analysis Working Paper 2000-9, Office of the Comptroller of the Currency, September 2000, USA
- The Internet and the National Bank Charter*, Comptroller of the Currency Administrator of National Banks, January 2001, USA
- Treatment of material on overseas Internet world wide web sites, accessible in the UK but not intended for investors in the UK*, Financial Services Authority, United Kingdom

Copyright 2003  
Information Systems Audit and Control Association  
3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Telephone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [research@isaca.org](mailto:research@isaca.org)  
Web Site: [www.isaca.org](http://www.isaca.org)