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 its vision. 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 ISACA 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.

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 CosiT™ 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 CosiT Framework. CosiT 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 (standards@isaca.org), faxed (+1.847.253.1443) or mailed (address at the end of procedure) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This material was issued on 1 July 2004.
1. **BACKGROUND**

1.1 **Linkage to Standards**

1.1.1 Standard S1 Audit Charter states, “The purpose, responsibility, authority and accountability of the information systems audit function or information system audit assignments should be appropriately documented in an audit charter or engagement letter.”

1.1.2 Standard S4 Professional Competence states, “The IS auditor should be professionally 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 comply with applicable laws and professional auditing standards.”

1.1.4 Standard S6 Performance of Audit Work states, “IS audit staff should be supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met”.

1.1.5 Procedure P8 Security Assessment—Penetration Testing and Vulnerability Analysis includes detailed steps when performing specific tests.

1.2 **Linkage to COBIT**

1.2.1 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 COBIT Management Guidelines provides 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 Management Guidelines provides 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 Management Guidelines can be used to support self-assessment workshops, and they can also 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 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 Mobile and wireless computing is a phenomenon that has begun to draw significant attention in worldwide business operations. Mobile and wireless computing refers to the use of wireless communication technologies to access network-based applications and information from a wide range of mobile devices. The increasing use of this technology and the proliferation of new portable devices with Internet browsing capabilities expand the physical frontiers of organisations and requires the IS auditor to understand this technology to identify the associated risks.

1.3.2 This guideline provides guidance in applying IS auditing standards S1, S4 and S5 when mobile computing security is to be reviewed as a part of an audit assignment or as an independent review. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgment in its application and be prepared to justify any departure.

2. **DEFINITIONS**

2.1 **Wireless Computing**

2.1.1 The term wireless computing refers to the ability of computing devices to communicate in a form to establish a local area network without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11x and other wireless standards and radio band services used by mobile devices.

2.2 **Mobile Computing**

2.2.1 The term mobile computing extends this concept to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. It is comprised of PDAs, cellular phones, laptops and other mobile and mobile-enabled technologies.

2.3 **Usage**

2.3.1 As devices that have computing and storage capability, mobile devices can be used to store, process and access applications and data in various ways. They can be used as semi-independent devices that process data in an independent form and periodically connect to a central system or a network to exchange data or applications with other systems, or they can be used as client nodes that access and/or update data stored in another remote system on a real-time basis (they may act as peers as well as in a hierarchy).
2.4 Approach

2.4.1 Mobile devices are computers that are ultimately formed by common components, such as hardware, operating system, applications and communications/connectivity links. This document covers those specific topics associated with an audit/review of the use of a device for mobile computing purposes. The inherent risks associated with the equipment and the rest of the environment are not covered in this document. (Examples of risk areas not covered are firewall configuration, viruses and program maintenance.)

3. TERMS OF REFERENCE

3.1 Scope

3.1.1 The IS auditor should have a clear statement of the objectives and scope of the audit to be performed in regards to mobile computing, which are ordinarily documented in an engagement letter.

4. PLANNING

4.1 Information Gathering

4.1.1 The IS auditor should obtain the security policy that rules the acceptable use of mobile devices.

4.1.2 The IS auditor should obtain information about the intended use of mobile devices, identifying where they are used for business transaction and data processing and/or for personal productivity purposes (i.e., Internet browsing, mail, calendar, address book, to-do list) and about hardware and software technologies used. Key processes—automated and manual—should be documented.

4.1.3 The IS auditor should obtain sufficient information about the risk analysis, along with the likelihood of occurrence and probable impact of the event, performed by the entity to evaluate the impacts of its mobile computing environment.

4.1.4 The IS auditor should obtain sufficient information about the policies and procedures used to manage mobile computing, involving deployment, operation and maintenance of aspects, such as communications, hardwar, application software, data security, systems software and security software. Examples of areas to cover are device configuration, physical control, approved software and tools, application security, network security, contingency plans, backup and recovery.

4.1.5 Personal interviews, documentation analysis (such as business case and protocols documentation) and wireless infrastructure testing should be used appropriately in gathering, analysing and interpreting the data.

4.1.6 Where third-party organisations are used to outsource IS or business functions, the IS auditor should review the terms of the agreement, evaluating the appropriateness of the security measures they enforce and the right of the organisation to periodically review the environment of the third party involved in the service it provides.

4.1.7 The IS auditor should also review previous examination reports and consider their results in the planning process.

4.2 Risk Analysis

4.2.1 The IS auditor should consider the risks associated with the use of mobile devices and relate them to the criticality of the information they store and access and the transactions they process, from the business, law and regulatory perspectives.

4.2.2 The portability, capability, connectivity and affordability of mobile devices enables them to be used to process applications that increase risks, such as:

- Damage, loss or theft (due to its portability)
- Damage to network assets by the transfer of viruses, worms, etc. from the mobile device.
- Unauthorised access to data by downloading data from corporate devices or networks (due to its connectivity)
- Unauthorised changes or additions to data by uploading data to corporate devices or networks
- Unauthorised access to data/applications that reside in the device (due to the simplicity of its operating systems that ordinarily include only very basic security functions)

4.2.3 Topics to consider when performing the risk analysis include:

- Privacy—An important component when sensitive information (such as, credit card numbers, financial details and patient records) is transmitted. Privacy protocols and related procedures are very important as wireless transmissions cannot be protected from hacker access by other means (such as physical access controls).
- Authentication—Can be ensured by using a token or certificate that can be verified by a recognised certification authority (CA)
- Two-factor authentication—Used to verify both the device and the identity of the end user during a secure transaction (i.e., confirms that both the device and the user are authorised agents). Two-factor authentication is used to deny network access from stolen or lost devices.
- Data integrity—Involves the detection of any change to the content of a message during the transmission or while stored on the mobile device.
- Nonrepudiation—A system to prevent users from denying they processed a transaction. Nonrepudiation requires a successful user authentication, and establishes a credible and legally enforceable record of the user that originated a transaction.
- Confidentiality and encryption—Involves transformation of data using algorithms to avoid unauthorised users or devices that could eventually read and understand it (see IS Auditing Procedure P9 Evaluation of Management Controls Over Encryption Methodologies). Encryption technologies rely on keys to encode and decipher pieces of data during transmission. Procedures for key distribution and safekeeping should also be considered.
- Unauthorised use of equipment and communications, including the risk of using unauthorised access to the Internet to break into a third-party’s networks (subjecting the entity to potential legal liability)
4.2.4 The IS auditor should assess the probability that the risks identified will materialise together with their likely effect, and document the risks along with the controls that mitigate these risks. Depending on the scope of the review, the IS auditor should include the most likely sources of threats—internal as well as external sources—such as hackers, competitors and alien governments.

4.3 IS Audit Objectives

4.3.1 According to the objectives and scope of the audit, the IS auditor should include in his/her review security areas, such as:

- Communications (covering risks such as sniffing and denial-of-service, and protocols such as encryption technologies and fault tolerance)
- Network architecture
- Virtual private networks
- Application delivery
- Security awareness
- User administration
- User and session administration (covering risk such as hijacking, spoofing, loss of integrity of data)
- Physical security
- Public key infrastructure
- Backup and recovery procedures
- Operations (such as incident response and back-office processing)
- Technology architecture (such as feasible, expandable to accommodate business needs and usable)
- Security architecture.
- Security software (such as IDS, firewall and antivirus)
- Security administration.
- Patch deployment
- Business contingency planning

4.4 Work Plan

4.4.1 Based on the information obtained and the scope and objectives of the engagement, the IS auditor has to document the way business, security and IS objectives (when applicable) are affected by the identified risks and controls that mitigate those risks.

4.4.2 In this process the IS auditor should evaluate areas of weakness or vulnerabilities that need strengthening. New controls identified as mitigating the risks considered should be included in a work plan for testing purposes.

5. PERFORMANCE OF AUDIT WORK

5.1 Execution

5.1.1 In the event of a lack of controls, the IS auditor should consider extending the planned procedures (for example including a penetration test) to identify the real vulnerabilities of the environment and test if they have not impacted on the objectives of the audit.

5.2 Reporting

5.2.1 The IS auditor should provide a report in an appropriate form to the intended service user recipients upon the completion of the audit work.

5.2.2 The IS auditor should consider discussing the report with the appropriate stakeholders prior to release.

5.2.3 The report should specify any restrictions on distribution that the IS auditor or management agree to impose. The IS auditor should also consider including a statement excluding liability to third parties.

6. EFFECTIVE DATE

6.1 This guideline is effective for all information systems audits beginning on or after 1 September 2004. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.

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 information criteria:

Primary
PO9—Assess Risks
AI3—Acquire and Maintain Technology Architecture
AI4—Develop and Maintain IT Procedures
AI5—Install and Accredit Systems
AI6—Manage Changes
DS5—Ensure Systems Security
DS9—Manage the Configuration
M2—Assess Internal Control Adequacy

Secondary
The CoBIT information criteria are confidentiality, integrity and availability, efficiency and reliability.