IS AUDITING GUIDELINE
RESPONSIBILITY, AUTHORITY AND ACCOUNTABILITY DOCUMENT G34

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. The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting. They 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
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements. 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.
- **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. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

CobiT® resources should be used as a source of best practice guidance. 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". 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.

As defined in the CobiT framework, each of the following is organised by IT management process. CobiT is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices and recommendations to be made around a commonly understood and well-respected standard reference. CobiT includes:

- 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. They 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? 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.
  - 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? 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 identify control gaps and strategies for improvement.

A glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*. The words audit and review are used interchangeably.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

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 Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to 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 document) to ISACA International Headquarters, for the attention of the director of research, standards and academic relations. This material was issued on 1 December 2005.

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 systems audit assignments should be appropriately documented in an audit charter or engagement letter".

1.1.2 Standard S3 Professional Ethics and Standards states, “The IS auditor should adhere to the ISACA Code of Professional Ethics”.

1.2 Linkage to CobiT

1.2.1 High-level control objective M3 (*Obtain independent assurance*) states, “…obtaining independent assurance to increase confidence and trust among the organisations, customers and third-party providers”.

1.2.2 High-level control objective M4 (*Provide for independent audit*) states, “…providing for independent audit to increase confidence levels and benefit from best practice advice”.

1.2.3 Detailed control objective M4.1 (*Audit charter*) states, “A charter for the audit function should be established by the organisation’s senior management. This document should outline the responsibility, authority and accountability of the audit function. The charter should be reviewed periodically to assure that the independence, authority and responsibility of the audit function are maintained”.

1.3 CobiT Reference

1.3.1 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 control objectives and associated management practices. To meet the requirement, the processes in CobiT most likely to be relevant, selected and adapted are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- M2—*Assess internal control adequacy.*
- M3—*Obtain independent assurance.*
- M4—*Provide for independent audit.*

1.3.3 Secondary:

- PO6—*Communicate management aims and direction.*
- PO7—*Manage human resources.*
- PO8—*Ensure compliance with external requirements.*
- DS1—*Define and manage service levels.*
- DS2—*Manage third-party services.*
- DS10—*Manage problems and incidents.*
- M1—*Monitor the process.*

1.3.4 The information criteria most relevant to responsibility, authority and accountability are:

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

1.4 Purpose of the Guideline

1.4.1 With continual increase in system complexity and correspondingly ingenious cyberthreats, organisations are increasingly looking to professionals who have the proven skill, expertise and knowledge to identify, evaluate and recommend solutions to mitigate system risks and vulnerabilities. IS auditors play a crucial role in responding to rapidly changing information technology, its associated vulnerabilities and potential exposures to protect the organisation’s assets and assist in risk identification, evaluation and mitigation. IS auditors provide technical IT skills and expertise to the audit function—whether external or internal—and there is an ever-increasing need to maintain an adequate level of skill and knowledge in IT expertise as the technological sophistication in financial and operational environment increases. In the present era, where technology is the prime business driver or a key enabler to support business processes, organisations and their stakeholders are relying on the IS auditor to determine whether management is committed to ensure the safeguarding of assets; data integrity, effectiveness and efficiency; adherence to corporate policies; and compliance with legal, regulatory and statutory obligations.

1.4.2 ISACA’s IS auditing standards and CobiT clearly emphasise that the audit charter should accurately establish the IS auditors responsibility, authority and accountability to conduct audits.

1.4.3 It is in this context that there is a need for a guideline to provide guidance to IS auditors on their responsibility, authority and accountability on accepting to conduct audit assignments.

1.4.4 This guideline provides guidance in applying IS Auditing Standards S1 Audit Charter and S3 Professional Ethics and Standards. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. RESPONSIBILITY

2.1 To the Profession

2.1.1 The IS auditor should be straightforward, honest and sincere in his/her approach to professional work.

2.1.2 The IS auditor should be independent of the auditee in attitude and appearance.

2.1.3 The IS auditor should adhere to the codes of professional ethics prescribed by his/her respective professional bodies, such as ISACA's Code of Professional Ethics

2.1.4 The IS auditor should conduct his/her activities in accordance with applicable auditing standards and generally accepted auditing practices applicable to the profession of IS auditing, such as ISACA's IS Auditing Standards, Guidelines and Procedures.

2.1.5 In instances where compliance is not achievable due to the circumstances of the audit environment, the IS auditor should disclose the fact of such non-compliance including the reason thereof and the effect on the audit of such non-compliance with applicable auditing standards in the audit report.

2.1.6 The IS auditor should uphold the dignity of the profession at all times.

2.1.7 The IS auditor should comply with applicable regulatory and statutory requirements.

2.1.8 The IS auditor should possess the required knowledge, competencies and skill to conduct accepted assignments.

2.1.9 The IS auditor should supervise all audit staff assigned to the IS audit, assure quality, comply with applicable standards and facilitate staff development.

2.1.10 The IS auditor should obtain and maintain sufficient and competent audit evidence in support of his/her conclusions and recommendations. In an audit of an information systems environment, some of the audit evidence may be in electronic form. The IS auditor should provide reasonable assurance that such audit evidence is adequately and safely stored and is retrievable in its entirety as and when required.

2.2 To the Auditee (Organisation)

2.2.1 The IS auditor should recognise, understand and assimilate the auditee's business objectives, goals and mission.

2.2.2 The IS auditor should understand the auditee's professional requirements of the IS auditor including, but not limited to, all independent requirements placed upon by the auditee.

2.2.3 Wherever appropriate, the IS auditor and auditee should mutually agree on the scope, objectives and terms of reference of the audit assignment.

2.2.4 The IS auditor should obtain sufficient understanding of management's attitudes, awareness and actions regarding internal controls and their importance to assess the appropriateness of the internal control environment.

2.2.5 The IS auditor should conduct a preliminary assessment of control risk relevant to activity under review. Audit objectives should reflect the results of this assessment. The IS auditor should document—in the audit working papers—the understanding obtained of the organisation's control systems and the assessment of control risk.

2.2.6 The IS auditor should use appropriate risk assessment techniques in developing the overall audit plan. When the control risk is assessed at a lower level, the IS auditor should also document the basis for the conclusions. In such an event, the IS auditor should obtain audit evidence through tests of control to support his/her assessment of control risk. The lower the assessment of control risk, the more audit evidence the IS auditor should obtain that IS/internal control systems are suitably designed and operating effectively.

2.2.7 Based on the results of the tests of control, the IS auditor should evaluate whether the internal controls are designed and operating as contemplated in the preliminary assessment of control risk. The IS auditor should consider the assessed levels of inherent and control risks in determining the nature, timing and extent of substantive procedures required to reduce audit risk to an acceptably low level.

2.2.8 The IS auditor should confirm the assessment of control risk based on results of substantive procedures and other audit evidence obtained during the conduct of the audit. In case of deviations from the prescribed control systems, the IS auditor should make specific inquiries to consider their implications. Where, on the basis of such inquiries, the IS auditor concludes that the deviations are such that the preliminary assessment of control risk is not supported; he/she should amend the same unless the audit evidence obtained from other tests of control supports that assessment. Where the IS auditor concludes that the assessed level of control risk needs to be revised, he/she should modify the nature, timing and extent of his/her planned substantive procedures.

2.2.9 The IS auditor should discuss with audit management and agree upon the audit plan, audit methodology, resources, time frame, and reporting requirements for the assignment. In planning the portions of the audit that may be affected by the IS environment, the IS auditor should obtain an understanding of the significance and complexity of the IS activities, appropriateness of stated controls and the availability and reliability of the data for use in the audit. This understanding would include such matters as:

- The information systems infrastructure [hardware, operating system(s) and application software used by the organisation, including changes, if any, therein since last audit]
- The significance and complexity of processing in each significant application
- Determination of the organisational structure of the organisation's IS activities and the extent of concentration or distribution of processing throughout the organisation, particularly, as they may affect segregation of duties
- Determination of the availability of data, reliability of available data, source documents, computer files and other audit evidence that may be required by the IS auditor and that may exist for only a short period or only in machine-readable form. Computer information systems may generate reports that might be useful in performing substantive tests (particularly analytical procedures).

2.2.10 The IS auditor should conduct the audit with due diligence and due professional care.

2.2.11 The IS auditor should have knowledge of key information technology risks and controls and available technology, such as computer assisted audit tools and other data analysis techniques, to perform his/her assigned work. Audits should be performed with proficiency and due professional care. The audit team collectively should possess or obtain the knowledge, skills and other competencies needed to perform their responsibilities.

2.2.12 The IS auditor should make management aware, as soon as practical and at an appropriate level of responsibility, of material weaknesses in the design or operation of the internal control systems that have come to the auditor's attention.

2.2.13 If the IS auditor believes that senior management has accepted a level of residual risk that may be unacceptable to the organisation, the IS auditor should discuss the matter with senior management. If the decision regarding residual risk is not resolved, the IS auditor should consider reporting the same to the board for resolution.

2.2.14 The IS auditor should respect the confidentiality of information acquired in the course of his/her work and should not disclose any such information to a third party without specific authority or unless there is a legal or professional duty to disclose it. The duty of confidentiality continues even after conclusion of the assignment and/or termination of the relationship between the IS auditor and the auditee.

2.2.15 The IS auditor should maintain an appropriate communication channel with the auditee. Communication should be accurate, objective, clear, concise, constructive, complete and timely. Results of the audit should be communicated to appropriate parties or authorities.

2.2.16 The IS auditor should submit a report in the appropriate form on completion of the audit. The report should include limitations, if any, on distribution and use of the results. The report should identify the organisation, the intended recipients and any restrictions on its circulation. The IS auditor should follow the reporting standards, policies and procedures of his/her respective audit organisations.

2.2.17 The IS auditor should be independent of the auditee at all times in attitude and appearance. The IS auditor's role is to audit an organisation's IS/internal policies, practices and procedures to assure that controls are adequate to achieve the organisation's mission. Although an IS auditor may be part of the organisation being audited, it is important and necessary that the IS auditor's independence be maintained.

2.2.18 In circumstance where the IS auditor is part of an organisation's control framework, he/she should provide reasonable assurance that he/she is not part of the team which is responsible for implementing specific IS/internal control procedures in the organisation under review.

2.2.19 The IS auditor should follow-up as appropriate and as required by the terms of assignment. If required, the IS auditor should also establish a follow-up process to monitor and determine that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2.3 To the Stakeholders

2.3.1 The IS auditor should serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.

2.3.2 The IS auditor should disclose all material instances or events that have a direct bearing on the stakeholders' interests.

2.3.3 The IS auditor should disclose the true and correct state of affairs of the area under audit, as per scope and objectives of assignment.

2.3.4 The IS auditor should avoid misstatements and/or ambiguous statements, or statements leading to varied interpretations, in the report.

2.3.5 The IS auditor should disclose instances of loss of independence, if any, during the conduct of the audit.

2.4 Statutory and Regulatory

2.4.1 The IS auditor should keep abreast with the applicable laws, rules and regulations.

2.4.2 The IS auditor should review compliance with applicable statutory laws, rules, regulations and contracts and, where applicable, seek legal guidance.

2.4.3 The IS auditor should disclose information as required by law and, where appropriate, with the consent of the auditee

2.4.4 The IS auditor should use licensed tools and software in conducting audit assignments.

2.5 To Society

2.5.1 The IS auditor should support the education of the public and auditees in enhancing their understanding of IS security, control, assessing and managing risks, safeguarding IS assets, etc.

2.5.2 The IS auditor should support the education of the public and auditees on the uses and possible abuses of technology, control models, control objectives, generally accepted control practices, monitoring and assuring methodologies.

2.5.3 The IS auditor should support the education of the public and auditees on the precautions to be undertaken and preventive measures to be considered where transactions happen with the aid of technology.

3. AUTHORITY

3.1 Rights of IS Auditors

3.1.1 The IS auditor has the right to have an engagement letter or audit charter specifying the scope, objective and terms of reference of the audit.

3.1.2 The IS auditor has the right to access appropriate information and resources to effectively and efficiently complete the audit.

3.1.3 The IS auditor has the right to believe that management has established appropriate controls to prevent, deter and detect fraud unless the tests and evaluation carried on by the IS auditor prove otherwise.

3.1.4 The IS auditor has the right to call for such information and explanations deemed necessary and appropriate to permit objective completion of the audit.

3.1.5 The IS auditor has the right to retain the working files, documents, audit evidences, etc., obtained during the course of the audit, in support of his/her conclusions and to use the same as the basis of reference in case of any issues or contradictions.

3.2 Limitations

3.2.1 The IS auditor should have sufficient knowledge to identify the indicators of fraud but may not be expected to have the expertise of the person whose primary responsibility is detecting and investigating fraud.

3.2.2 The IS auditor should apply the due professional care and skill expected of a reasonably prudent and competent professional. However, due professional care does not imply infallibility.

3.2.3 The IS auditor should be alert to the significant risks that might affect objectives, operations or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

3.2.4 Where the IS auditor is not able to obtain required information, is restricted from accessing resources or is in any way restrained from carrying out his/her function, the IS auditor should escalate his/her concerns to appropriate senior levels in management. The IS auditor should conduct the audit in a professional manner.

3.2.5 Where the IS auditor has utilised the services of an external expert, the IS auditor should evaluate the usefulness and sufficiency of work performed by such external expert and also perform appropriate testing to confirm the findings of the external expert.

3.2.6 The IS auditor is not responsible for implementing corrective actions.

4. ACCOUNTABILITY

4.1 Professional Accountability

4.1.1 Conventional interpretation and ordinary discourse interpret accountability as a process of assigning blame and punishing wrongdoing. Professionally, this should be seen as a positive incentive—as an opportunity to demonstrate achievements and stewardship. In this view, accountability is an integral and indispensable part of establishing effective relationships for getting things done and owning responsibility.

4.1.2 The IS auditor's precise role and relationship varies with different organisations and the nature of the assignment. Therefore, it is important that there is clarity over whom the assignment serves and the purpose of the assignment. The auditor's relationship with each of the key parties should be determined and documented in the engagement letter with the auditee.

4.1.3 It is generally accepted in principle that the IS auditor should be objective and thus remain independent from organisation management. The board or management often seek greater reassurance about controls and other matters. It is management's responsibility to establish and maintain adequate internal control structure. In such circumstances, the IS auditor is accountable for the credibility of the submitted report.

4.1.4 Accountability can be established through due professional diligence, a proactive approach, transparency in the delivery of services, and reporting/providing credible and timely information to the concerned/recognised group.

4.1.5 Accountability is responsibility for performance against agreed-upon expectations both stated or implied.

4.1.6 The IS auditor should exercise due caution from disclosing information acquired in the course of his/her professional engagement to any person other than the organisation, without consent of the organisation or otherwise than as required by any statute for the time being in force. The IS auditor should always keep in view the various regulatory and statutory issues applicable to the organisation audited to provide reasonable assurance of the compliance with disclosure of information.

4.2 Professional Negligence

4.2.1 The IS auditor should not express an opinion without obtaining sufficient and competent information and possessing relevant audit evidence based upon generally accepted auditing practices.

4.2.2 The IS auditor should report to appropriate parties/authorities any material departure from procedures, policies and compliance matters that has come to his/her notice during the conduct of the assignment.

4.3 Restrictions

4.3.1 The IS auditor should not accept assignments if his/her independence will be impaired or perceived to be impaired. For example, if the IS auditor has a beneficial interest in the auditee organisation or is not independent of the auditee, he/she should not accept the assignment. Instances of beneficial interest may be indebtedness to or significant investment in the organisation.

4.3.2 The IS auditor should not allow any unauthorised person or firm to conduct IS audit assignments in his/her name.

4.3.3 The IS auditor should not solicit professional work by unfair means and not make payment of commission or brokerage for obtaining professional assignments.

4.3.4 The IS auditor should not advertise his/her professional accomplishments or services. In promoting themselves and their professional services, IS auditors should:

- Not use means which brings disrepute to the profession
- Not make exaggerated claims for the services offered, qualifications possessed or experience gained
- Not denigrate work of other IS auditors

4.3.5 The IS auditor should not seek professional work by unethical means.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning 1 March 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

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: *standards@isaca.org*
Web site: *www.isaca.org*