

IS AUDITING GUIDELINE

COMPETENCE

DOCUMENT G30

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 judgement 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 to identify control gaps and strategies for improvement.

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 15 February 2005.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S4 Professional Competence states, "The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment. The IS auditor should maintain professional competence through appropriate continuing professional education and training."

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 amongst 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 M3.7 (Competence of Independent Assurance Function) states, "Management should ensure that the independent assurance function possesses the technical competence, skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner."

1.2.4 Detailed control objective M4.4 (Competence) states, "Management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to information systems auditing tasks maintain technical competence through appropriate continuing professional education".

1.3 CoBIT Reference

1.3.1 The CoBIT references offer the specific objectives or processes of CoBIT to consider when reviewing the area addressed by this guidance. 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 likely to be the most relevant are selected and adapted and 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:

- PO7—Manage Human Resources
- M2—Assess Internal Control Adequacy
- M3—Obtain Independent Assurance
- M4—Provide for Independent Audit

1.3.3 Secondary:

- DS1—Define and Manage Service Levels
- DS2—Manage Third Party Services
- DS3—Manage Performance and Capacity
- DS7—Educate and Train Users
- M1—Monitor the Process

1.3.4 The information criteria most relevant to competence are:

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

1.4 Purpose of the Guideline

1.4.1 IS auditors are expected to be highly competent. To meet this objective, IS auditors need to acquire the necessary skills and required knowledge to carry out assignments. The additional challenge is to maintain competence by continually upgrading knowledge and skills.

1.4.2 By agreeing to provide professional services, IS auditors imply the availability of the desired level of competence required to perform professional services and that the knowledge and skill of the IS auditor will be applied with due care and diligence.

1.4.3 In view of the expectations of high competence, IS auditors should refrain from performing any services that they are not competent to carry out unless advice and assistance is obtained to provide reasonable assurance that the services are performed satisfactorily.

1.4.4 The IS auditor should perform professional services with due care, competence and diligence and has a continuing duty to maintain professional knowledge and skill at a required level to provide reasonable assurance that the requirements of professional auditing standards are met and the audited organisation receives the advantage of competent professional service based on up-to-date developments in practice, legislation and techniques.

1.4.5 ISACA's stated vision is to be the recognised global leader in IT governance, control and assurance. In the preface to the vision, it is clearly amplified that future success in the professions served by ISACA will require skills and competencies complementary to those measured by the CISA designation. ISACA is in the forefront of identifying these skills and competencies and devising ways to quantify and assess them. It is in this context that there is a need for a guideline to provide guidance to IS auditors to acquire necessary skills and knowledge and maintain competence while carrying out audit assignments.

1.4.6 This guideline provides guidance in applying IS auditing standard S4 Professional Competence. 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 Skills and Knowledge

2.1.1 Primarily, the IS auditor should be responsible for acquiring the required professional and technical skills and knowledge to carry out any assignment the IS auditor agrees to perform.

2.1.2 Audit management has the secondary responsibility to entrust the audit assignment after ensuring that the IS auditor possesses the required professional and technical skills and knowledge to perform the tasks.

2.1.3 Audit management is responsible for ensuring that the team members performing the audit have the requisite skills and knowledge.

2.1.4 Skills and knowledge vary with the IS auditor's position and the role with respect to the audit. Requirement for management skills and knowledge should be commensurate with the level of responsibility

2.1.5 Skills and knowledge include proficiency in the identification and management of risks and controls, as well as audit tools and techniques. The IS auditor should possess analytical and technical knowledge together with interviewing, interpersonal and presentation skills.

2.2. Competence

2.2.1 Competence implies possessing skills and knowledge, and expertise through an adequate level of education and experience.

2.2.2 The IS auditor should provide reasonable assurance that he/she possesses the skills and knowledge necessary to attain the required level of competence.

2.2.3 The IS auditor should design the desired and/or expected level of competence based on appropriate benchmarks and such benchmarks are periodically reviewed and updated.

2.2.4 IS auditor and/or audit management should provide reasonable assurance of the availability of competent resources required to carry out any audit assignment prior to accepting the assignment/engagement, and the availability of such competent resources should be confirmed/ensured prior to commencement of an audit.

2.2.5 Audit management is responsible for ensuring the team members are competent to perform the audit assignment. Identification of core competencies of team members will assist in efficient utilisation of available resources.

2.2.6 It is considered appropriate for the IS auditors to share their experiences, adopted best practices, lessons learned and knowledge gained amongst team members to improve the competence of the resources. The competence of team members is also improved through team building sessions, workshops, conferences, seminars, lectures and other modes of interaction.

2.3 Continual Maintenance

2.3.1 The IS auditor should continually monitor their skills and knowledge to maintain the acceptable level of competence.

2.3.2 Maintenance through continuing professional education (CPE) may include, and is not limited to, training, educational courses, certification programmes, university courses, conferences, seminars, workshops, teleconferences, web casts and study circle meetings.

2.3.3 Acquiring skills and knowledge and maintaining competence levels should be monitored on a continual basis, and such skills, knowledge and competence should be evaluated periodically.

2.4 Evaluation

2.4.1 Evaluation should be carried out in a manner that is fair, transparent, easily understood, unambiguous, without bias and considered a generally acceptable practice given the respective employment environment.

2.4.2 Evaluation criteria and procedures should be clearly defined, but may vary depending upon circumstances such as geographic location, political climate, nature of assignment, culture and other similar circumstances.

2.4.3 In the case of an audit firm or a team of auditors, evaluation should be carried out internally amongst teams or individuals on a cross-functional basis.

2.4.4 In the case of a single (sole) independent IS auditor, evaluation should be carried out by a peer relationship to the extent possible. If a peer review is not possible, self-evaluation should be conducted and documented.

2.4.5 An appropriate level of management is required to evaluate the performance of the internal IS auditor and also, wherever appropriate and necessary, the performance of external IS auditor(s).

2.4.6 Gaps noted during evaluation should be addressed appropriately.

2.5 Gap Analysis and Training

2.5.1 Gaps noted based upon variances in the actual level of competence to the expected level of competence should be recorded and analysed. Where deficiency exists in any resource, such resources should not be utilised to conduct the audit assignment unless adequate measures to rectify the deficiency are undertaken. However, if the deficiency is noticed after commencement of the audit assignment, the IS auditor/audit management should consider withdrawing the deficient resource(s) and replacing it with a competent resource. However due to compulsions, if it is proposed to continue to use the resource for the continuance of the audit assignment, the existence of the gap should be communicated to the auditee. The concurrence of the auditee should be obtained for the continued use of the deficient resource, provided that the IS auditor is able to reasonably assure the quality of the audit.

2.5.2 It is important that the root cause analysis is performed to ascertain the reason for the gap and that appropriate corrective action measures, such as training, are conducted as soon as possible.

2.5.3 Training activities required for an audit engagement should be completed within a reasonable time and before commencement of the audit activity.

2.5.4 Effectiveness of training should be measured on completion of training after a reasonable time period.

2.6 Availability of Competent Resources

2.6.1 The IS auditor/audit management should understand and analyse the requirement of skills and knowledge of the proposed audit assignment, before responding to a request for proposal.

2.6.2 The IS auditor/audit management should provide reasonable assurance that requisite resources with the necessary skills, knowledge and required level of competency are available before commencing the audit assignments.

2.6.3 IS auditors should not portray themselves as having expertise, competence or experience they do not possess.

2.7 Outsourcing

2.7.1 Where any part of the audit assignment is outsourced or expert assistance obtained, it must be reasonable assurance must be provided that the external expert or the outsourced agency possesses the requisite competence. This guideline also applies for selection of an external expert.

2.7.2 Where expert assistance is obtained on a continual basis, competencies of such external experts should be measured and monitored/reviewed periodically.

3. CONTINUING PROFESSIONAL EDUCATION

3.1 Requirements of Professional Bodies

3.1.1 Continuing professional education (CPE) is the methodology adopted to maintain competence and update skills and knowledge.

3.1.2 IS auditors should adhere to the requirements of the CPE policies established by the respective professional bodies with which they are associated.

3.2 Eligible Programmes

3.2.1 CPE programmes should aid in the enhancement of skill and knowledge and must relate to professional and technical requirements of IS assurance, security and governance

3.2.2 Professional bodies ordinarily prescribe programmes eligible for CPE recognition. IS auditors should adhere to such norms prescribed by their respective professional bodies.

3.3 Attainment of CPE credits

3.3.1 Professional bodies ordinarily prescribe the methodology of attainment of CPE credits and the minimum credits that should be obtained periodically by their constituents. IS auditors must adhere to such norms prescribed by their respective professional bodies.

3.3.2 Where the IS auditor is associated with more than one professional body for the purpose of attainment of minimum credits, the IS auditor may use his/her judgement to avail CPE credits in a common manner from the eligible programmes, provided the same is consistent with the rules/guidelines framed by the respective professional bodies.

3.4 ISACA's CPE Policy

3.4.1 ISACA has a comprehensive policy on continuing professional education, applicable to its members and holders of the CISA designation. IS auditors with the CISA designation must comply with ISACA's CPE policy. Details of the policy are available on the ISACA web site, www.isaca.org/CISAcpePolicy. The policy explains the criteria for:

- Certification requirements
- Verification of attendance form
- Code of Professional Ethics
- Audits of continuing professional education hours
- Revocation, reconsideration and appeal
- Retired and nonpracticing CISA status
- Qualifying educational activities
- Calculating continuing professional education hours

4. RECORDS

4.1 Skill Matrix and Training Records

4.1.1 A skill matrix indicating the skill, knowledge and competence required for various job levels should be formulated. This matrix is cross-referenced to the available resources and their skill and knowledge. This matrix will aid in the identification of gaps and training needs.

4.1.2 Records of training provided, together with feedback on training and effectiveness of training, should be maintained, analysed and referenced for future use.

4.2 CPE Records

4.2.1 As prescribed by respective professional bodies, including ISACA, IS auditors are required to maintain appropriate records of CPE programmes, retain them for specific periods and, if required, make them available for audits.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning 1 June 2005. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.

Information Systems Audit and Control Association 2004-2005 Standards Board

Chair, Sergio Fleginsky, CISA	PricewaterhouseCoopers, Uruguay
Svein Aldal	Aldal Consulting, Norway
John Beveridge, CISA, CISM, CFE, CGFM, CQA	Office of the Massachusetts State Auditor, USA
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP	Value Partners, Italy
Christina Ledesma, CISA, CISM	Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP	Brisbane City Council, Australia
V. Meera, CISA, CISM, ACS, CISSP, CWA	Microsoft Corporation, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Ikanos Communications, India
Peter Niblett, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Thomas Thompson, CISA	Ernst & Young, UAE

© Copyright 2005
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