

G12 ORGANISATIONAL RELATIONSHIP AND INDEPENDENCE

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 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.

Control Objectives for Information and related Technology (CobIT[®]) is published by the IT Governance Institute[®] (ITGI[™]). It is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. CobIT enables clear policy development and good practice for IT control throughout organisations. It emphasises regulatory compliance, helps organisations increase the value attained from IT, enables alignment and simplifies implementation of the CobIT framework's concepts. CobIT is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. CobIT is available for download on the ISACA web site, www.isaca.org/cobit. As defined in the CobIT framework, each of the following related products and/or elements is organised by IT management process:

- **Control objectives**—Generic statements of minimum good control in relation to IT processes
- **Management guidelines**—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
 - Performance measurement
 - IT control profiling
 - Awareness
 - Benchmarking
- **CobIT Control Practices**—Risk and value statements and 'how to implement' guidance for the control objectives
- **IT Assurance Guide**—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

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 in the IS Auditing Standards, Guidelines and Procedures.

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 all 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 IT 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 July 2008.

1. BACKGROUND

1.1 Linkage to Standards

- 1.1.1 Standard S2 Independence states: 'In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance'.
- 1.1.2 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'.
- 1.1.3 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 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 independence requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary.
- 1.2.2 PO4 *Define the IT processes, organisation and relationships* satisfies the business requirement for IT of being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes.
- 1.2.3 Secondary references:
 - ME2 *Monitor and evaluate internal control*
 - ME4 *Provide IT governance*
- 1.2.4 The information criteria most relevant are:
 - Primary: Effectiveness and efficiency
 - Secondary: Confidentiality, integrity, availability, compliance and reliability

1.3 Need for Guideline

- 1.3.1 The purpose of this guideline is to expand on the meaning of 'independence' as used in standard S2 and to address the IS auditor's attitude and independence in IS auditing.
- 1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. INDEPENDENCE

2.1 Attitude

- 2.1.1 IS auditors should seek adherence to applicable codes of professional ethics and auditing standards in all of their work.
- 2.1.2 As per COBIT, the audit charter should ensure that the independence, authority and accountability of the audit function are maintained and established by appropriate members of the organisation's management team.

3. PLANNING

3.1 Staffing

- 3.1.1 The IS auditor establishes many relationships with people involved in the audit activity and has the opportunity to explore the innermost aspects of the area being audited, often the whole organisation. The IS auditor's attitude should always be appropriate to this role. Planning should take into account any known relationships.
- 3.1.2 IS auditors should not participate in an audit if their independence is impaired. For example, independence is impaired if IS auditors have some expectation of financial gain or other personal advantage due to their influence on the results of the audit. However, the IS auditors' independence would not necessarily be impaired as a result of performing an audit of IS where their personal transactions occur in the normal course of business.
- 3.1.3 At the beginning of the audit, IS auditors may be required to sign a conflict-of-interest statement to declare their independence.

3.2 Prioritised Audit Plan

3.2.1 COBIT process ME4 states: 'Management should provide for independent audit'. To achieve this objective, an audit plan should be established. This plan should verify that regular and independent assurance is obtained regarding the effectiveness, efficiency and economy of security and internal control procedures. Within this plan, management should determine priorities regarding obtaining independent assurance.

4. PERFORMANCE OF AUDIT WORK

4.1 Organisation

4.1.1 IS auditors should be organisationally independent of the area being audited. Independence is impaired if the IS auditors have direct control over the area being audited. The IS auditors' independence can also be impaired if the IS auditors have direct reporting responsibility to those individuals who have direct control over the area being audited. The IS auditors' independence also may be impaired if IS auditors are required, for tracking purposes, to report their time expended in performing the audit, including progress, audit issues, etc., to the IT group responsible for those controls tested and who report the results to senior or executive management. This could be perceived as the IT group project managing the IS auditors and, thus, an impairment of the IS auditors' independence. In addition, IS auditors should take into consideration if independence has been impaired in situations where the scope of work performed is based on requirements of the control process owners for business or regulatory purposes.

4.1.2 Independence should be regularly assessed by the IS auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. IS auditors should consider the use of control self-assessment techniques in this continuous assessment process.

4.1.3 Depending on the assignment, IS auditors can interview persons, analyse organisational processes, gain assistance from the organisation's staff, etc. An IS auditor's attitude and appearance of independence should always be adequate to meet these situations. IS auditors should be aware that the appearance of independence can be influenced by their actions or associations. Perceptions of the IS auditors' independence could affect the acceptance of their work.

4.1.4 If IS auditors become aware that a situation or relationship is perceived to impair their independence, they should inform audit management of the perceived impairment as soon as possible.

4.2 Gathering Information

4.2.1 Amongst the various items needed to obtain an understanding of the organisation being audited, IS auditors, to preserve their independence, should review:

- Organisation policies and procedures relating to the independent assurance process
- Audit charter, mission statement, policies, procedures and standards, prior reports, and audit plans
- The organisational chart

4.3 Controls Evaluation

4.3.1 IS audit plans should define the activities from which IS auditors are required to be independent. IS auditors' independence from these activities should be regularly monitored by senior management, or by the person who determines and approves IS audit plans. This monitoring should include an assessment of the process for assigning individual IS auditors to specific assignments, to verify that this process assures independence and sufficient skills.

4.3.2 Verification of the IS auditors' adherence to applicable professional codes of conduct should always be carried out. In many circumstances, this should be sufficient to provide audit evidence of independence. If there is an indication that an IS auditor's independence has been compromised, a revision of the audit plan should be considered.

5. REPORTING

5.1 Effect on Reporting

5.1.1 In circumstances where the IS auditor's independence is impaired and the IS auditor continues to be associated with the audit, the facts surrounding the issue of the IS auditor's independence should be disclosed to the appropriate management and in the report.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning on or after 1 September 2000. The guideline has been reviewed and updated effective 1 August 2008.

2007-2008 ISACA Standards Board	
Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Capco IT Services India Private Ltd., India
Brad David Chin, CISA, CPA	Google Inc., USA
Sergio Fleginsky, CISA	AKZO Nobel, Uruguay
Maria Gonzalez, CISA, CISM	Department of Defence, Spain
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew J. MacLeod, CISA, FCPA, MACS, PCP, CIA	Brisbane City Council, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Jason Thompson, CISA	KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA

ISACA
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