

G1 USING THE WORK OF OTHER EXPERTS

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 an information technology (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 February 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S13 Using the Work of Other Experts states 'The IS auditor should, where appropriate, consider using the work of other experts for the audit'.

1.1.2 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'.

1.2 Linkage to COBIT

1.2.1 ME2.5 states that the IS auditor should 'Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews. Such reviews may be conducted by the corporate compliance function or, at management's request, by internal audit or commissioned to external auditors and consultants or certification bodies. Qualifications of individuals performing the audit, e.g., CISA[®] certification, must be ensured.'

1.3 Need for Guideline

1.3.1 The interdependency of customers' and suppliers' processing and the outsourcing of non-core activities mean that an IS auditor (internal or external) will often find that parts of the environment being audited are controlled and audited by other independent functions or organisations. This guideline sets out how the IS auditor should comply with the above standard in these circumstances. Compliance with this guideline is not mandatory, but the IS auditor should be prepared to justify deviation from it.

1.3.2 IS auditors should consider using the work of other experts in the audit when there are constraints that could impair the audit work to be performed or potential gains in the quality of the audit. Examples of these are the knowledge required by the technical nature of the tasks to be performed, scarce audit resources and limited knowledge of specific areas of audit. An 'expert' could be an IS auditor from the external accounting firm, a management consultant, an IT expert or expert in the area of the audit who has been appointed by top management or by the IS audit team. An expert could be internal or external to an organisation as long as independence and objectivity is maintained.

2. AUDIT CHARTER

2.1 Rights of Access to the Work of Other Experts

2.1.1 The IS auditor should verify that, where the work of other experts is relevant to the IS audit objectives, the audit charter or engagement letter specifies the IS auditor's right of access to this work.

3. PLANNING

3.1 Planning Considerations

3.1.1 When the IS auditor does not have the required skills or other competencies to perform the audit, the IS auditor should seek competent assistance from other experts; however, the IS auditor should have good knowledge of the work performed but not be expected to have a knowledge level equivalent to the experts.

3.1.2 When an IS audit involves using the work of other experts, the IS auditor should consider their activities and their effect on the IS audit objectives whilst planning the IS audit work. The planning process should include

- Assessing the independence and objectivity of the other experts
- Assessing their professional competence and qualifications
- Obtaining an understanding of their scope of work, approach, timing and quality control processes, including assessing if they exercised due care in creating working papers and retaining evidence of their work
- Determining the level of review required

3.2 Independence and Objectivity

3.2.1 The processes for selection and appointment, the organisational status, the reporting line and the effect of their recommendations on management practices are indicators of the independence and objectivity of other experts.

3.3 Professional Competence

3.3.1 The qualifications, experience, resources and credentials of other experts should all be taken into account in assessing professional competence.

3.4 Scope of Work and Approach

3.4.1 Scope of work and approach ordinarily will be evidenced by the other expert's written audit charter, terms of reference or letter of engagement.

3.5 Level of Review Required

3.5.1 The nature, timing and extent of audit evidence required will depend upon the significance and scope of the other expert's work. The IS auditor's planning process should identify the level of review that is required to provide sufficient reliable, relevant and useful audit evidence to achieve the overall IS audit objectives effectively. The IS auditor should review the other expert's final report, audit programme(s) and audit work papers. The IS auditor should also consider whether supplemental testing of the other expert's work is required.

4. PERFORMANCE OF AUDIT WORK

4.1 Review of Other Expert's Work Papers

4.1.1 The IS auditor should have access to all work papers created by the expert, supporting documentation and reports of other experts, where such access does not create legal issues.

4.1.2 Where the expert's access to records creates legal issues and, hence, such access is not available, the IS auditor should appropriately determine and conclude the extent of use and reliance on the expert's work.

4.1.3 In reviewing other expert's work papers, the IS auditor should perform sufficient audit work to confirm that the other expert's work was appropriately planned, supervised, documented and reviewed, to consider the appropriateness, sufficiency of the audit evidence provided by them, and to determine the extent of use and reliance on the expert's work. Compliance with relevant professional standards should also be assessed. The IS auditor should assess whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives and document such conclusion.

4.1.4 Based on the assessment of the work of other experts' work papers, the IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts does not provide sufficient and appropriate audit evidence.

4.1.5 If additional test procedures performed do not provide sufficient and appropriate audit evidence, the IS auditor should provide appropriate audit conclusion and include scope limitation where required.

4.2 Review of Other Expert's Report(s)

4.2.1 The IS auditor should perform sufficient reviews of the other expert's final report(s) to confirm that the scope specified in the audit charter, terms of reference or letter of engagement has been met; that any significant assumptions used by the other experts have been identified; and that the findings and conclusions reported have been agreed upon by management.

4.2.2 It may be appropriate for management to provide their own report on the audited entities, in recognition of their primary responsibility for systems of internal control. In this case, the IS auditor should consider management's and the expert's reports together.

4.2.3 The IS auditor should assess the usefulness and appropriateness of reports issued by the other experts, and should consider any significant findings reported by the other experts. It is the IS auditor's responsibility to assess the effect of the other expert's findings and conclusions on the overall audit objective, and to verify that any additional work required to meet the overall audit objective is completed

4.2.4 If an expert is engaged by another part of the organisation, reliance may be placed on the report of the expert. In some cases this may lessen the need for IS audit coverage even though the IS auditor does not have access to supporting documentation and work papers. The IS auditor should be cautious in providing an opinion on such cases.

4.2.5 The IS auditor's views/comments on the adoptability and relevance of the expert's report should form a part of the IS auditor's report if the expert's report is utilised in forming the IS auditor's opinion.

5. FOLLOW-UP ACTIVITIES

5.1 Implementation of Recommendations

5.1.1 Where appropriate, the IS auditor should consider the extent to which management has implemented any recommendations of other experts. This should include assessing if management has committed to remediation of issues identified by other experts within appropriate time frames and the current status of remediation.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning on or after 1 June 1998. The guideline has been reviewed and updated and is effective 1 March 2008.

2007-2008 ISACA Standards Board

Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Capco IT Services India Private Limited, India
Brad David Chin, CISA, CPA Google Inc., USA
Sergio Fleginsky, CISA ICI Paints, Uruguay
Maria Gonzalez, CISA HomeLand Office, Spain
John Ho Chi, CISA, CISM, CBCP, CFE Ernst & Young, Singapore
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australia
John G. Ott, CISA, CPA AmerisourceBergen, USA
Jason Thompson, CISA, CIA 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