ISACA® Serving IT Governance Professionals

IS AUDITING GUIDELINE

G2 AUDIT EVIDENCE REQUIREMENT

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 15 March 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 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’.

1.1.2 Standard S9 Irregularities and Illegal Acts states ‘The IS auditor should obtain sufficient and appropriate evidence to determine whether management or others within the organization have knowledge of actual, suspected or alleged irregularities and illegal acts’.

1.1.3 Standard S13 Using the Work of Other Experts states ‘The IS auditor should provide appropriate audit opinion and include scope limitation where required evidence is not obtained through additional test procedures’.

1.1.4 Standard S14 Audit Evidence states ‘The IS auditor should obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the audit results. The IS auditor should evaluate the sufficiency of audit evidence obtained during the audit‘.

1.1.5 Procedure P7 Irregularities and Illegal Acts states “Although the IS auditor has no explicit responsibility to detect or prevent irregularities, the IS auditor should assess the level of risk that irregularities could occur. The result of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during the engagement’.

1.2 Linkage to COBIT

1.2.1 ME2.3 *Control exceptions* states ‘Record information regarding all control exceptions and ensure that it leads to analysis of the underlying cause and to corrective action. Management should decide which exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Management is also responsible to inform affected parties’.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to guide the IS auditor to obtain sufficient and appropriate audit evidence and draw reasonable conclusions on which to base the audit results.

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 standard, use professional judgement in its application and be prepared to justify any departure.

2. PLANNING

2.1 Types of Audit Evidence

2.1.1 For a description of appropriate, reliable and sufficient evidence, refer to the commentary section in standard S14.

2.1.2 When planning the IS audit work, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. Amongst the things to be considered are the independence and qualifications of the provider of the audit evidence. For example, corroborative audit evidence from an independent third party can be more reliable than audit evidence from the organisation being audited. Physical audit evidence is generally more reliable than the representations of an individual.

2.1.3 The IS auditor should also consider whether testing of controls has been completed and attested to by an independent third party and whether any reliance can be placed on that testing.

2.1.4 The various types of audit evidence that the IS auditor should consider using include:

- Observed processes and existence of physical items
- Documentary audit evidence
- Representations
- Analysis

2.1.5 Observed processes and existence of physical items can include observations of activities, property and IS functions, such as:

- An inventory of media in an offsite storage location
- A computer room security system in operation

2.1.6 Documentary audit evidence, recorded on paper or other media, can include:

- Results of data extractions
- Records of transactions
- Program listings

- Invoices
- Activity and control logs
- System development documentation

2.1.7 Representations of those being audited can be audit evidence, such as:

- Written policies and procedures
- System flowcharts
- Written or oral statements

2.1.8 The results of analysing information through comparisons, simulations, calculations and reasoning can also be used as audit evidence. Examples include:

- Benchmarking IS performance against other organisations or past periods
- Comparison of error rates between applications, transactions and users

2.2 Availability of Audit Evidence

2.2.1 The IS auditor should consider the time during which information exists or is available in determining the nature, timing, extent of substantive testing and, if applicable, compliance testing. For example, audit evidence processed by electronic data interchange (EDI), document image processing (DIP) and dynamic systems such as spreadsheets may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up. Documentation availability could also be impacted by company document retention policies.

2.3 Selection of Audit Evidence

2.3.1 The IS auditor should plan to use the most appropriate, reliable and sufficient audit evidence attainable and consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence.

2.3.2 Where audit evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, the IS auditor should consider obtaining documentary confirmation of the representations, either on paper or other media. The auditor should also consider alternative evidence to corroborate these representations to ensure their reliability.

3. PERFORMANCE OF AUDIT WORK

3.1 Nature of Audit Evidence

3.1.1 Audit evidence should be sufficient, reliable, relevant and useful to form an opinion or support the IS auditor’s findings and conclusions. If, in the IS auditor’s judgement, the audit evidence obtained does not meet these criteria, the IS auditor should obtain additional audit evidence. For example, a program listing may not be adequate audit evidence until other audit evidence has been gathered to verify that it represents the actual program used in the production process.

3.2 Gathering Audit Evidence

3.2.1 Procedures used to gather audit evidence vary depending on the information system being audited. The IS auditor should select the most appropriate, reliable and sufficient procedure for the audit objective. The following procedures should be considered:

- Inquiry
- Observation
- Inspection
- Confirmation
- Reperformance
- Monitoring

3.2.2 The above can be applied through the use of manual audit procedures, computer-assisted audit techniques, or a combination of both. For example:

- A system which uses manual control totals to balance data entry operations might provide audit evidence that the control procedure is in place by way of an appropriately reconciled and annotated report. The IS auditor should obtain audit evidence by reviewing and testing this report.
- Detailed transaction records may only be available in machine-readable format requiring the IS auditor to obtain audit evidence using computer-assisted audit techniques. The auditor should ensure that the version or type(s) of computer-assisted audit techniques (CAATs) to be used are updated and/or fully compatible with the format(s) structured for the detailed transaction records in question.

3.2.3 If there is a possibility that the gathered evidence will become part of a legal proceeding, the IS auditor should consult with the appropriate legal counsel to determine whether there are any special requirements that will impact the way evidence needs to be gathered, presented and disclosed.

3.3 Audit Documentation

3.3.1 Audit evidence gathered by the IS auditor should be appropriately documented and organised to support the IS auditor's findings and conclusions.

3.3.2 For a discussion on protection and retention of evidence, refer to the commentary section in standard S14.

4. REPORTING

4.1 Restriction of Scope

4.1.1 In those situations where the IS auditor believes sufficient audit evidence cannot be obtained, the IS auditor should disclose this fact in a manner consistent with the communication of the audit results.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning on or after 1 December 1998. The guideline has been reviewed and updated effective 1 May 2008.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *standards@isaca.org*
Web Site: *www.isaca.org*