IS AUDITING GUIDELINE

G3 USE OF COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATs)

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 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 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 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 January 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 the appropriate analysis and interpretation of this evidence'.

1.1.2 Standard S5 Planning states 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.3 Standard S3 Professional Ethics and Standards states 'The IS auditor should exercise due professional care, including observance of applicable professional auditing standards'.

1.1.4 Standard S7 Reporting states 'The IS auditor should have sufficient and appropriate audit evidence to support the results reported'.

1.1.5 Standard S14 Audit Evidence states 'The IS auditor should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results'.

1.2 Linkage to Guidelines

1.2.1 Guideline G2 Audit Evidence Requirement provides guidance to the IS auditor regarding the type and sufficiency of audit evidence used in IS auditing.

1.2.2 Guideline G10 Audit Sampling provides guidance to the IS auditor regarding the design and selection of an audit sample and evaluation of sample results.

1.3 Linkage to COBIT

1.3.1 ME2 *Monitor and evaluate internal control* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.3.2 DS5 *Ensure systems security* satisfies the business requirement for IT of maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents by focusing on defining IT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents.

1.4 Need for Guideline

1.4.1 As entities increase the use of information systems to record, transact and process data, the need for the IS auditor to utilise IS tools to adequately assess risk becomes an integral part of audit coverage. The use of computer-assisted audit techniques (CAATs) serves as an important tool for the IS auditor to evaluate the control environment in an efficient and effective manner. The use of CAATs can lead to increased audit coverage, more thorough and consistent analysis of data, and reduction in risk.

1.4.2 CAATs include many types of tools and techniques, such as generalised audit software, customised queries or scripts, utility software, software tracing and mapping, and audit expert systems.

1.4.3 CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Penetration testing

1.4.4 CAATs may produce a large proportion of the audit evidence developed on IS audits and, as a result, the IS auditor should carefully plan for and exhibit due professional care in the use of CAATs.

1.4.5 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.

1.4.6 This guidance should be applied in using CAATs regardless of whether the auditor concerned is an IS auditor.

2. PLANNING

2.1 Decision Factors for Using CAATs

2.1.1 When planning the audit, the IS auditor should consider an appropriate combination of manual techniques and CAATs. In determining whether to use CAATs, the factors to be considered include:

- Computer knowledge, expertise, and experience of the IS auditor
- Availability of suitable CAATs and IS facilities
- Efficiency and effectiveness of using CAATs over manual techniques
- Time constraints
- Integrity of the information system and IT environment
- Level of audit risk

2.2 CAATs Planning Steps

2.2.1 The major steps to be undertaken by the IS auditor in preparing for the application of the selected CAATs include the following:

- Set the audit objectives of the CAATs, which may be included in the terms of reference for the exercise.
- Determine the accessibility and availability of the organisation's IS facilities, programs/systems and data.
- Clearly understand composition of data to be processed including quantity, type, format and layout.
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation).
- Define output requirements.
- Determine resource requirements, i.e., personnel, CAATs, processing environment (the organisation's IS facilities or audit IS facilities).
- Obtain access to the organisation's IS facilities, programs/systems and data, including file definitions.
- Document CAATs to be used, including objectives, high-level flowcharts and run instructions.

2.3 Arrangements with the Auditee

2.3.1 Adequate time may be needed from data owners or users to properly design the CAAT and interpret the data. In addition, the auditee should understand the purpose, scope, timing and goals of the CAATs. Setting clear expectations at the outset of the CAAT should be communicated.

2.3.2 Data files, such as detailed transaction files, are often only retained for a short period of time; therefore, the IS auditor should make arrangements for the retention of the data covering the appropriate audit time frame.

2.3.3 Access to the organisation's IS facilities, programs/systems and data should be arranged well in advance of the needed time period to minimise the effect on the organisation's production environment, if possible.

2.3.4 The IS auditor should assess the effect that changes to the production programs/systems may have on the use of CAATs. In doing so, the IS auditor should consider the effect of these changes on the integrity and usefulness of CAATs, as well as the integrity of the programs/systems and data used by the IS auditor.

2.4 Testing the CAATs

2.4.1 It is critical that the IS auditor obtain reasonable assurance of the integrity, reliability, usefulness and security of the CAATs through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed on CAATs. The nature, timing and extent of testing is dependent on the commercial availability and stability of the CAATs. Custom CAATs should receive additional review and testing to ensure CAATs are operating as expected.

2.5 Security of Data and CAATs

2.5.1 Where CAATs are used to extract information for data analysis, the IS auditor should verify the integrity of the information system and IT environment from which the data are extracted.

2.5.2 CAATs can be used to extract sensitive program/system information and production data that should be kept confidential. The IS auditor should clearly understand company data classification and data handling policies to properly safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the IS auditor should consider the level of confidentiality and security required by the organisation owning the data and any relevant legislation, and should consult others, such as legal counsel and management, as necessary.

2.5.3 The IS auditor should use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness and security of the CAATs. For example, this should include a review of program maintenance and program change controls over embedded audit software to determine that only authorised changes have been made to the CAATs.

2.5.4 When CAATs reside in an environment not under the control of the IS auditor, an appropriate level of control should be in effect to identify changes to the CAATs. When CAATs are changed, the IS auditor should obtain assurance of their integrity, reliability, usefulness and security through appropriate planning, design, testing, processing and review of documentation before reliance is placed on the CAATs.

3. PERFORMANCE OF AUDIT WORK

3.1 Gathering Audit Evidence

3.1.1 The use of CAATs should be controlled by the IS auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. The IS auditor should:

- Perform a reconciliation of control totals if appropriate
- Review output for reasonableness
- Perform a review of the logic, parameters or other characteristics of the CAATs
- Review the organisation's general IS controls, which may contribute to the integrity of the CAATs (e.g., program change controls and access to system, program, and/or data files)

3.1.2 When using test data, the IS auditor should be aware that test data only point out the potential for erroneous processing; this technique does not evaluate actual production data. The IS auditor should also be aware that test data analysis can be extremely complex and time consuming, depending on the number of transactions processed, the number of programs tested and the complexity of the programs/systems. Before using test data the IS auditor should verify that the test data will not permanently affect the live system.

3.2 Generalised Audit Software

3.2.1 When using generalised audit software to access the production data, the IS auditor should take appropriate steps to protect the integrity of the organisation's data. With embedded audit software, the IS auditor should be involved in system design and techniques should be developed and maintained within the organisation's application programs/systems.

3.3 Utility Software

3.3.1 When using utility software, the IS auditor should confirm that no unplanned interventions have taken place during processing and that the utility software has been obtained from the appropriate system library. The IS auditor should also take appropriate steps to protect the integrity of the organisation's system and files since these utilities can easily damage the system and its files.

3.4 Customised Queries or Scripts

3.4.1 Customised queries or scripts allow the IS auditor to specifically target desired information for analysis. Customised scripts are highly useful for environments where other CAATs are not available but usually require specific technical skill sets to create them. Therefore, the IS auditor should obtain assurance of their integrity, reliability, usefulness and security through appropriate planning, design and testing before reliance is placed on CAATs, and ensure that proper source data are used and that output from scripts and queries are in the proper format. Customised query and script code should be maintained in a secure location to prevent unauthorised changes from occurring.

3.5 Application Software Tracing and Mapping

3.5.1 When using application software tracing and mapping, the IS auditor should confirm that the source code being evaluated has generated the object program currently being used in production. The IS auditor should be aware that application software tracing and mapping only points out the potential for erroneous processing; it does not evaluate actual production data.

3.6 Audit Expert Systems

3.6.1 Audit expert systems are specialised tools that can be used to analyse the flow of data, through the processing logic of the application software, and document the logic, paths, control conditions and processing sequences. When using audit expert systems, the IS auditor should be thoroughly

knowledgeable of the operations of the system to confirm that the decision paths followed are appropriate to the given audit environment/situation.

3.7 Continuous Monitoring and Assurance

3.7.1 Continuous assurance is an uninterrupted monitoring approach that allows management and IS auditors to monitor controls on a continuous basis and to gather selective audit evidence through the computer. It is a process that can be used to provide immediate (or nearly so) reporting by IS auditors and lends itself to use in high-risk, high-volume environments. In the current audit model (used by both internal and external auditors), a period of time passes between the completion of fieldwork and issuance of the related audit report. In many instances, the impact of this delay in issuance makes the information contained in the report less useful or beneficial to the user. This is a result of the aging of the information contained in the report that can be affected by such issues as auditee corrections to identified deficiencies, further deterioration to the control environment (or related auditee data) resulting from identified control weaknesses or deficiencies.

3.7.2 Continuous assurance is therefore designed to enable IS auditors to report on subject matter within a much shorter time frame than under the current model. Theoretically, in some environments it should be possible to shorten the reporting time frame to provide almost instantaneous or truly continuous assurance.

3.7.3 By definition, continuous assurance requires a higher degree of reliance on an auditee's information systems than traditional auditing requires. This is a result of the need to rely upon system-generated information vs. externally produced information as the basis for audit testing. Hence, auditors need to make judgements on both the quality of the auditee's systems as well as the information produced by the system itself. Systems that are of lower quality, or produce less-reliable information, (and require a higher degree of manual intervention) are less conducive to continuous assurance than those that are of high quality and produce reliable information.

3.7.4 Environments that are of a higher quality and produce reliable information are better suited to reporting periods of a short to continuous duration. Environments that are of a lower quality or produce less-reliable information should use longer reporting periods to compensate for the period of time that must pass for users to review and approve or correct information processed by the system.

4. CAATs DOCUMENTATION

4.1 Workpapers

4.1.1 The step-by-step CAATs process should be sufficiently documented to provide adequate audit evidence.

4.1.2 Specifically, the audit workpapers should contain sufficient documentation to describe the CAATs application, including the details set out in the following sections.

4.2 Planning

4.2.1 Documentation should include:

- CAATs objectives
- CAATs to be used
- Controls to be exercised
- Staffing and timing

4.3 Execution

4.3.1 Documentation should include:

- CAATs preparation and testing procedures and controls
- Details of the tests performed by the CAATs
- Details of inputs (e.g., data used, file layouts), testing periods, processing (e.g., CAATs high-level flowcharts, logic) and outputs (e.g., log files, reports)
- Listing of relevant parameters or source code

4.4 Audit Evidence

4.4.1 Documentation should include:

- Output produced
- Description of the audit analysis work performed on the output

- Audit findings
- Audit conclusions
- Audit recommendations

4.4.2 Data and files used should be stored in a secure location. In addition, temporary confidential data used as part of the audit should be properly disposed in accordance with corporate data handling procedures

5. REPORTING

5.1 Description of CAATs

5.1.1 The objectives, scope and methodology section of the report should contain a clear description of the CAATs used. This description should not be overly detailed, but it should provide a good overview for the reader.

5.1.2 The description of CAATs used should also be included in the body of the report, where the specific finding relating to the use of CAATs is discussed.

5.1.3 If the description of the CAATs used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report, and the reader should be referred to an appendix with a more detailed description.

6. EFFECTIVE DATE

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

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: *http://www.isaca.org*