Information Systems Audit and Control Association

IS AUDITING GUIDELINE

USE OF COMPUTER ASSISTED AUDIT TECHNIQUES (CAATs)

Introduction

The specialised nature of information systems auditing, and the skills necessary to perform such audits, require globally applicable standards that apply specifically to information systems auditing. One of the Information Systems Audit and Control Association, Inc.'s (ISACA's) goals is therefore to advance standards to meet this need. The development and dissemination of Standards for Information Systems Auditing are a cornerstone of the ISACA's professional contribution to the audit community.

Objectives

The objectives of the ISACA's Standards for Information Systems Auditing are to inform

- Information Systems Auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the Code of Professional Ethics for Information Systems Auditors
- Management and other interested parties of the profession's expectations concerning the work of practitioners

The objective of IS Auditing Guidelines is to provide further information on how to comply with the Information Systems Auditing Standards.

Scope and Authority of Standards for Information Systems Auditing

The framework for the ISACA's Information Systems Auditing Standards provides for multiple levels of standards, as follows:

Standards define mandatory requirements for IS auditing and reporting.

Guidelines provide guidance in applying IS auditing standards. The IS Auditor should consider them in determining how to achieve implementation of the above standards, use professional judgment in their application and be prepared to justify any departure.

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 doing information systems auditing work, but do not set requirements.

The ISACA Code of Professional Ethics requires members of the ISACA and holders of the Certified Information Systems Auditor (CISA) designation to comply with Information Systems Auditing Standards adopted by the ISACA. Apparent failure to comply with these may result in an investigation into the member's or CISA holder's conduct by the ISACA Board or appropriate ISACA committee and disciplinary action may ensue.

Development of Standards, Guidelines and Procedures

The ISACA Standards Board is committed to wide consultation in the preparation of Information Systems 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 on-going development programme, and would welcome the input of members of the ISACA and holders of the CISA designation to identify emerging issues requiring new standards products. Any suggestions should be e-mailed (research@isaca.org) or faxed (+1.847. 253 .1443) to ISACA's International Office, for the attention of the Director of Research, Standards and Academic Relations.

Withdrawal of Previously Issued Documents

This Guideline replaces the previously issued Statement on Information Systems Auditing Standard Number 9 on "Use of Audit Software Tools". SISAS 9 will be withdrawn on 1 December 1998.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard 060.020 (Evidence) states "During the course of the audit, the Information Systems Auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.2 Standard 050.010 (Audit Planning) states "The Information Systems Auditor is to plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards."

1.1.3 Standard 030.020 (Due Professional Care) states "Due professional care and observance of applicable professional auditing standards are to be exercised in all aspects of the Information Systems Auditor's work."

1.2 Need for Guideline

1.2.1 Computer Assisted Audit Techniques (CAATs) are important tools for the IS Auditor in performing audits.

1.2.2 CAATs include many types of tools and techniques, such as generalised audit software, utility software, test data, application software tracing and mapping, and audit expert systems.

1.2.3 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

1.2.4 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.

1.2.5 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 judgment in its application and be prepared to justify any departure.

1.2.6 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 are:

- Set the audit objectives of the CAATs
- Determine the accessibility and availability of the organisation's IS facilities, programs/system and data
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation, etc.)
- Define output requirements
- Determine resource requirements, i.e., personnel, CAATs, processing environment (organisation's IS facilities or audit IS facilities)
- Obtain access to the organisation's IS facilities, programs/system, 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 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.

2.3.2 Access to the organisation's IS facilities, programs/system, and data, should be arranged for well in advance of the needed time period in order to minimise the effect on the organisation's production environment.

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

2.4 Testing the CAATs

2.4.1 The IS Auditor should 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 upon the CAATs. The nature, timing and extent of testing is dependent on the commercial availability and stability of the CAATs.

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 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.

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 were made to the CAATs.

2.5.4 When the 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 the 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)

3.2 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 the techniques will have to 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 Test Data

3.4.1 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 also should 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/system. Before using test data the IS Auditor should verify that the test data will not permanently affect the live system.

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 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 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.

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), 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

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 the CAATs used should also be included in the body of the report, where the specific finding relating to the use of the 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 referred to an appendix with a more detailed description.

6. EFFECTIVE DATE

6.1 This Guideline is effective for all information systems audits beginning on or after 1 December 1998.

APPENDIX - GLOSSARY

Application Software Tracing and Mapping – 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. Both the command language or job control statements and programming language can be analysed. This technique includes program/system: mapping, tracing, snapshots, parallel simulations, and code comparisons.

Audit Expert Systems – expert or decision support systems that can be used to assist IS Auditors in the decision-making process by automating the knowledge of experts in the field. This technique includes automated risk analysis, system software, and control objectives software packages.

Computer Assisted Audit Techniques (CAATs) – any automated audit techniques, such as generalised audit software, utility software, test data, application software tracing and mapping, and audit expert systems.

Generalised Audit Software – a computer program or series of programs designed to perform certain automated functions. These functions include reading computer files, selecting data, manipulating data, sorting data, summarising data, performing calculations, selecting samples, and printing reports or letters in a format specified by the IS Auditor. This technique includes software acquired or written for audit purposes and software embedded in production systems.

Test Data – simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications. Individual programs or an entire system can be tested. This technique includes Integrated Test Facilities (ITFs) and Base Case System Evaluations (BCSEs).

Utility Software – computer programs provided by a computer hardware manufacturer or software vendor and used in running the system. This technique can be used to examine processing activity, test programs, system activities and operational procedures, evaluate data file activity, and analyse job accounting data.

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
Email: research@isaca.org
Web Site: http://www.isaca.org