STATEMENT 3.262

AUDITING GUIDELINE

COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATs)

Introduction

1. Paragraphs 11 to 13 of Auditing Guideline No. 3.260 "Auditing in an EDP environment — general principles" indicates that:

   (a) the application of compliance and substantive procedures may require the use of CAATs; and

   (b) the effectiveness and efficiency of audit procedures may be improved through the use of CAATs.

2. When an audit is conducted in an EDP environment the application of audit procedures may require the auditor to adopt techniques that use the computer as an audit tool. These various uses of the computer are known as Computer-Assisted Audit Techniques (CAATs).

3. The purpose of this Guideline is to provide guidance in the use of CAATs. This Guideline applies to all uses of CAATs when a computer of any type or size is involved, whether that computer is operated by the entity or by a third party (for example, a computer service bureau).

Description of CAATs

4. **The principles expressed in this statement apply to the use of all CAATs.** Examples of CAATs together with some of their advantages and disadvantages have been included in the Appendix to this guideline for information. Historically, audit software used to interrogate a client's financial data files and test data for audit purposes have been regarded as the most popular and widely used CAATs, and detailed descriptions of these have been incorporated in this guideline. The impact of advancing technology has caused an increase in the usage of many of the other techniques mentioned in the Appendix, particularly where they relate to general controls. However, these techniques are generally similar in nature to audit software and test data and therefore have not been described in detail within the main statement.

Audit software

5. Audit software consists of computer programs used by the auditor, as part of the audit procedures, to process data of audit significance from the EDP system. It may consist of generalised audit software, specialised audit software or utility programs and existing entity programs.

   a. Generalised audit software consists of package computer programs designed to perform a variety of data processing functions such as to read computer files, select desired information, perform calculations and print reports in a format specified by the auditor.

   b. Specialised audit software refers to computer programs designed to perform audit tasks in specific circumstances. These programs may be prepared by the auditor, by the entity or by an outside programmer engaged by the auditor.

   c. Utility programs and existing entity programs are used by the entity to perform common data processing functions such as sorting, creating and printing computer files. These computer programs are not usually designed for audit purposes and therefore may not contain such features as automatic record counts or control totals.

Test data

6. Test data techniques are methods of conducting audit procedures by entering data (for example, a sample of transactions) into the EDP system, and comparing the results obtained with pre-determined results. Examples of this are outlined below.

   a. Test data can be developed by the auditor to test specific controls in computer programs, such as on-line password and data access controls.

   b. Test data in the form of test transactions can be selected from previously processed transactions or can be created by the auditor to test specific programmed procedures of the computer program. These test transactions are generally processed separately from normal processing.

c. Test data in the form of test transactions can be used in a "live" mode, where a dummy unit (for example, a department or employee) is established to which test transactions are posted during normal processing. This technique, when integrated into normal processing so as to operate on a continuous basis over a period of time, is known as an "integrated test facility" (ITF). When using this technique, the auditor should ensure that the impact of test transactions is subsequently eliminated from the computer files.

Uses of CAATs

7. CAATs may be used during various audit procedures, such as:

(a) detailed testing of transactions and balances (for example, the use of audit software to test all or a sample of the transactions in a computer file);

(b) analytical review (for example, the use of audit software to identify unusual fluctuations or items);

(c) compliance testing of EDP application controls (for example, the use of test data to check the functioning of a programmed procedure);

(d) testing of general EDP controls (for example, to analyse logs and to review program library access procedures).

Considerations in the use of CAATs

8. When planning the audit, the auditor should consider an appropriate selection of manual and/or computer-assisted audit techniques. When determining whether to use CAATs and which CAATs to select, the factors to be considered include:

(a) the computer knowledge, expertise and experience of the auditor;

(b) the reliability of general EDP controls;

(c) the availability of CAATs and suitable EDP facilities;

(d) the impracticability of manual audit procedures;

(e) effectiveness and efficiency; and

(f) timing.

Computer knowledge, expertise, and experience of the auditor

9. The level of skills and knowledge necessary for the planning and use of CAATs varies considerably. As a minimun, where the auditor is using audit software to achieve straightforward audit objectives with simple detailed specifications, he should have a knowledge of data processing and the computer applications together with a detailed knowledge of the audit software and computer files to be used. Where applications are complex, the auditor should have an appreciation of systems analysis, operating systems and experience of the software language to be utilized by the auditor.

Reliability of general EDP controls

10. The auditor's review of the accounting system and related internal controls should include a preliminary evaluation and identification of the general EDP controls necessary to ensure the integrity of CAATs. Where his preliminary evaluation indicates that the general EDP controls may be unreliable there is a risk that the integrity of CAATs may be compromised. Depending on the extent of the weaknesses in general EDP controls, the auditor should consider alternative procedures, such as:

    (a) performing substantive tests (e.g. log analysis) on the areas of weakness in general controls to determine the actual impact of the weaknesses on the CAATs;

    (b) requesting the establishment of compensating control procedures to strengthen the areas of weakness, at least for the period during which CAATs are used;

    (c) copying the relevant data and processing CAATs at an alternative facility.

Availability of CAATs and suitable EDP facilities

11. The auditor should consider the availability of CAATs and EDP facilities and the accessibility of any necessary EDP systems or computer files. He may plan to use other EDP facilities when the use of CAATs on the entity's EDP facilities is inefficient, impractical, or where he cannot exercise sufficient control over the processing of CAATs.

12. The co-operation of the entity's personnel will usually be required to provide EDP facilities at a convenient time, to assist with such activities as the loading and running of the CAATs on the EDP system and to provide copies of computer files in the format required by the auditor. It is appropriate for the auditor to use CAATs on copies of computer files and programs provided that he has taken steps to gain reasonable assurance that the copy is identical with the original.

Impracticability of manual audit procedures

13. Many EDP systems perform tasks for which no documentary evidence is available and, in these circumstances, it may not be practical for the auditor to perform procedures manually. Where such procedures are significant to the audit process, CAATs may have to be used. The lack of visible evidence may occur at different stages in the accounting process as outlined below.

    (a) The absence of input documents (for example, order entry in on-line systems) or the generation of accounting transactions by computer programs (for example, automatic calculation of discount or interest) may preclude the auditor from examining documentary evidence and authorization of individual transactions.

    (b) The transient nature of processing may preclude the auditor from manually following transactions or the application of controls through the EDP system. For example, delivery notes and suppliers' invoices may be matched by a computer program; edit routines and programmed procedures, such as checking customer credit limits and validity tests, may provide visible evidence only on an exception basis. In such cases, there may be no documentary evidence that all transactions have been processed, edited or controlled.

    (c) The lack of hardcopy output and the retention of data only in machine readable form may preclude the effective performance of manual audit procedures. For example, a printed report may contain summary totals and not supporting details.

Effectiveness and efficiency

14. The effectiveness and efficiency of audit procedures may be improved through the use of CAATs to obtain and evaluate audit evidence, for example:

    (a) some transactions may be tested more effectively and/or efficiently by using CAATs to examine all or a greater number of transactions in a computer file than would otherwise be selected;

(b) in applying analytical review procedures, transaction or balance details may be reviewed and reports of unusual items printed more efficiently than by manual methods; and

(c) the use of CAATs may make substantive procedures more efficient than placing reliance on controls and related compliance procedures.

15. Matters which contribute to the effectiveness and efficiency of CAATs include:

(a) time to plan, design, test, execute and evaluate CAATs;

(b) availability of technical assistance and review requirements;

(c) availability of computer time; and

(d) stability of the EDP systems and application software.

In evaluating the effectiveness and efficiency of CAATs the auditor should consider the life span of the application. Developing CAATs during the initial planning and design stages of an application may also benefit audits in subsequent periods.

Timing

16. Certain computer files, such as detailed transaction files, may be retained only for a short time, and may not be available in machine readable form when required by the auditor. Thus, it may be necessary to make arrangements for the retention of data required or to alter the timing of the audit work which requires this data.

17. Where the time available to perform an audit is limited the auditor may plan to use CAATs because it will meet the time requirement more efficiently than other audit procedures.

Using CAATs

18. Following the decision to use CAATs the auditor should ensure that their use is properly controlled and documented.

19. The major steps to be undertaken by the auditor in the application of CAATs are to:

(a) identify the objectives;

(b) determine the content and accessibility of the entity's computer files;

(c) define the transaction types to be tested;

(d) define the procedures to be performed on the data;

(e) define the output requirements;

(f) identify the audit and computer personnel who will participate in the design and application of CAATs;

(g) reconsider effectiveness and efficiency;

(h) determine the controls to be applied by the auditor in relation to the integrity of data files, programs or techniques involved;

(i) organise the administrative activities, including the necessary skills and computer facilities;

(j) carry out the CAATs; and

(k) evaluate the results and perform the necessary audit tests on them.

Controlling the use of CAATs

20. The use of CAATs should be controlled by the auditor to provide reasonable assurance that the audit objectives and the detailed specifications of CAATs have been met, and that CAATs are not improperly manipulated. This control requires the auditor to:

(a) approve the technical specifications, and carry out a technical review of the work involving the use of CAATs;

(b) consider the entity's general EDP controls which may contribute towards the integrity of CAATs, for example, controls over access to computer files and over program changes; and

(c) ensure appropriate integration of the output by the auditor into the audit process.

21. When using CAATs the auditor will usually require the co-operation of the computer staff, as they will have extensive knowledge of the EDP system. In such circumstances the auditor should have reasonable assurance that the computer staff do not improperly influence the results of CAATs. The level of audit assurance that the auditor can derive from the results of CAATs is directly related to the degree of independence achieved in their use.

22. Regardless of whether audit software is prepared by the auditor, the entity's own programming personnel or by an outside programmer engaged by the auditor, the auditor should actively participate in:

    (a) defining or, where appropriate, reviewing the objectives of that audit software;

    (b) supervising any development or maintenance; and

    (c) testing the software.

23. Procedures to be carried out by the auditor in order to control audit software applications include:

    (a) developing or supervising the development of the audit software;

    (b) running the audit software on small test files with predetermined results before running it on the main computer files;

    (c) ensuring that the correct computer files are used (for example, by reviewing external evidence such as manual control totals and the operating system and instruction log);

    (d) obtaining evidence that the audit software has functioned as planned (for example, by the review of output and control information);

    (e) considering the storage of the source and object versions of CAATs to ensure the integrity of those computer programs;

    (f) ensuring CAATs do not alter the entity's computer files; and

    (g) ensuring the security of the entity's computer files when they are removed from the entity's premises.

    Although proper control of audit software applications does not necessarily require the auditor to be present during computer runs in order to control distribution of output and to ensure the timely correction of errors, there may be practical advantages to this (for example where the wrong input file is used).

24. In order to control test data applications, the auditor should:

    (a) supervise and control the submissions of test data;

    (b) compare the actual test data output with the predetermined results for the individual transactions and in total;

(c) confirm that the authorized production version of the computer programs was used to process the test data; and

(d) evaluate the changes made to the computer program during the audit period to determine the effect on test data results.

Documentation

25. The audit working papers should record the work done using CAATs and the conclusions reached. It may be convenient to keep the technical papers relating to the use of CAATs separate from the other audit working papers, but wherever they are maintained the standard of working papers and retention procedures should be consistent with that of the audit as a whole.

26. The working papers should contain sufficient documentation to describe the application of CAATs, such as:

(a) planning

(i) CAATs objectives;

(ii) specific CAATs used;

(iii) controls to be exercised;

(iv) staffing and timing;

(b) execution

(i) details of the procedures performed by CAATs;

(ii) CAATs preparation and testing procedures and controls;

(iii) details of input, processing and output;

(iv) relevant technical information about the EDP system;

(c) audit evidence

(i) output;

(ii) description of the audit procedures performed on the output;

(iii) conclusions reached on the audit objectives;

(d) other

(i) recommendations to management;

(ii) suggestions for future years.

Appendix I

EXAMPLES OF COMPUTER-ASSISTED AUDIT TECHNIQUES

NB: The following examples, which are in alphabetical order, require varying degrees of technical skill.

Techniques	*Description*	*Advantages*	*Disadvantages*
Audit Software	Software used by the auditor to read data on client's files, to provide information for the audit and/or to re-perform procedures carried out by the client's programs	· Performs a wide variety of audit tasks · Long term economies · Reads actual records · Capable of dealing with large volumes	· Requires a degree of skill to use · Initial set up costs can be high · Adaptation often needed from machine to machine
Core Image Comparison	Software used by the auditor to compare the executable version of a program with a secure master copy	· Provides a high degree of comfort concerning the executable version of the program · Particularly useful where only executable versions are distributed	· Requires a high degree of skill to set up and to interpret the results · Where programs have been recompiled the comparison may be invalidated as the program records everything as a difference · Printouts are hard to interpret and the actual changes made are difficult to establish · Availability restricted to certain machine types
Database Analysers	Software used by the auditor to examine the rights associated with terminals and the ability of users to access information on a database	· Provides detailed information concerning the operation of the database · Enhances the auditor's understanding of the database management system	· Requires a high degree of skill to set up and to interpret the results · Restricted availability both as regards machine types and database management systems · Specific and limited audit applicability

Techniques	*Description*	*Advantages*	*Disadvantages*
Embedded Code	Software used by the auditor to examine transactions passing through the system by placing his own program in the suite of programs used for processing	· Performs a wide variety of audit tasks · Examines each transaction as it passes through the system · Operates continuously · Capable of identifying unusual transactions passing through the system	· There is a processing overhead involved because of the extra programs · Definition of what constitutes an unusual transaction needs to be very precise · Precautions need to be taken over the output from the programs to ensure its security · Precautions need to be taken to ensure that the program cannot be suppressed or tampered with · Requires some degree of skill to use and to interpret the results
Log Analysers	Software used by the auditor to read and analyse records of machine activity	· Provides detailed information on machine usage · Long term economies · Effective when testing integrity controls	· Requires a high degree of skill to use and to interpret the results · Limited availability as regards machine types · High volume of records restricts extent of test
Mapping	Software used by the auditor to list unused program instructions	· Identifies program code which may be there for fraudulent reasons	· Very specific objective · Requires a high degree of skill to use and to interpret the results · Adaptation needed from machine to machine

Techniques	*Description*	*Advantages*	*Disadvantages*
Modelling	A variety of software, usually associated with a microcomputer, enabling the auditor to carry out analytical reviews of client's results, to alter conditions so as to identify amounts for provisions or claims, or to project results and compare actual results with those expected	· Can be a very powerful analytical tool · Can enable the auditor to examine provisions on a number of different bases · Very flexible in use · Can provide the auditor with useful information on trends and patterns	· A high volume of data may need to be entered initially · Results require careful interpretation
On-line Testing	Techniques whereby the auditor arranges or manipulates data either real or fictitious, in order to see that a specific program or screen edit test is doing its work	· Very widely applicable · Easy to use · Can be targetted for specific functions carried out by programs	· Each use satisfies only one particular objective · Care must be taken to ensure that "live" data does not impact actual results
Program Code Analysis	An examination by the auditor of the source code of a particular program with a view to following the logic of the program so as to satisfy himself that it will perform according to his understanding	· Gives a reasonable degree of comfort about the program logic · The auditor can examine every function of the program code	· The auditor must understand the program language · The auditor needs to check that the source code represents the version in the source library, and that this version equates to the executable version

Techniques	*Description*	*Advantages*	*Disadvantages*
Program Library Analysers	Software used by the auditor to examine dates of changes made to the executable library and the use of utilities to amend programs	· Provides the auditor with useful information concerning the program library · Identifies abnormal changes to the library · Useful when testing program security	· Requires a high degree of skill to use and to interpret the results · Availability restricted to certain machine types · Only relevant when testing integrity controls
Snapshots	Software used by the auditor to take a "picture" of a file of data or a transaction passing through the system at a particular point in time	· Permits the auditor to examine processing at a specific point in time to carry out tests, or to confirm the way a particular aspect of the system operates	· Can be expensive to set up
Source Comparison	Software used by the auditor to compare the source version of a program with a secure master copy	· Compares source code line by line and identifies all differences · Useful when testing integrity controls or particularly important program procedures	· Other procedures are necessary to ensure that the executable version reflects the source code examined · Requires some degree of skill to use and to interpret the results · Availability restricted to certain machine types

Techniques	*Description*	*Advantages*	*Disadvantages*
Test Data — "Live", "Dead", Integrated Test Facility or Base Case System Evaluation	Fictitious data applied against the client's programs either whilst they are running or in an entirely separate operation. The results of processing the fictitious data are compared with the expected results based on the auditor's understanding of the programs involved	· Performs a wide variety of tasks · Gives considerable comfort about the operation of programs · Can be precisely targetted for specific procedures within programs · Long term economies	· "Dead" test data requires additional work for the auditor to satisfy himself the right programs were used · Care must be taken to ensure that "live" data does not impact actual results · Technique can be expensive to set up and cumbersome to use · Adequate for detection of major error but less likely to detect deep-seated fraud
Tracing	Software used by the auditor to identify which instructions were used in a program and in what order	· Helps to analyse the way in which a program operates	· There may be cheaper ways to achieve the same objectives, although not in the same detail · Requires a high degree of skill to use and to interpret the results · Adaptation needed from machine to machine