TOPIC 47: THE USE OF COMPUTER ASSISTED AUDIT TECHNIQUES (CAATS)

Computer Based Auditing

- Introduction
- GENERAL COMPUTER INFORMATION SYSTEM CONTROLS
  - Application Controls: “Abs Spec”
- How do auditors use computers in performing audits?
- CAATS (Computer Assisted Audit Techniques)
- Considerations Affecting Use of CAATS
- Auditing Around the Computer
Introduction

COMPUTER-ASSISTED AUDIT TECHNIQUES - CAATs

Auditing in a Computer Information Systems (CIS) environment.

Auditors all over the world now use computers to a greater or lesser extent, and the proportion of their clients without a single PC is very small. So once again, the subject is important in practice as well as in theory. It should be noted that this is an area of constant change and evolution. We have already covered the internal controls expected within a manual system and additional controls will be required for the computer Information System.

Features and risks involved in auditing in a CIS environment?

CIS Factors

(i) Consistency of performance
Consistency of performance is both a strength and a weakness. Computer systems are more reliable than manual systems. A properly programmed application will process transactions consistently accurately, a program with errors will make errors consistently.

(ii) Concentration of knowledge, programs and data files
The number of computer specialists involved in a CIS environment will generally be low. In small organisations, there might only be one individual with a detailed knowledge of the functioning of the system as a whole. Such individuals are in a position to alter programs and data, and potentially conceal fraud. Transaction, master-file and program data are often held together, which increases the potential for unauthorised access. (Weak Segregation of Duties!)

Performing proper risk assessments may be difficult for an audit firm that employs very few computer specialists.

(iii) Ease of access to data and programs
This problem can be particularly acute where data can be altered from remote terminals.
There is still a widespread belief that computers and the records contained on them are inherently safer, and less vulnerable to loss and corruption than manual systems, where in fact the reverse is true.

(iv) Automatically generated transactions

Most systems are capable of generating transactions without human intervention. For example, bank interest is almost always charged automatically. The lack of authorisation and documentation can be a significant audit issue if many transactions are generated this way.

(v) Lack of source documentation and audit trail

Computers do not show handwriting, and the proper authorisation and attribution of transactions processed is correspondingly important. Many systems report by exception only, and this can make an audit trail difficult to follow if there is no hard copy of all transactions processed.

(vi) Programmed controls

Programmed controls are generally not visible and therefore need to be tested indirectly, or using test data. There may also be a belief that general IT controls are unimportant, or inexpensive.

(vii) Vulnerability of storage media

The data stored is highly vulnerable to loss, corruption, theft and destruction – i.e. theft of laptops.

(viii) Multiple update of files

Incorrect entries, particularly when encoded, may result in incorrect data in many different accounts, particularly in database systems.

Acquisition of network

(i) Before the change

The system will need to be assessed and tested as normal.

(ii) The changeover to the New System
The auditor must ensure that all records have been properly removed from the old system and entered into the new one. This will probably involve the use of control/Batch totals (Arithmetical Control), but may be complicated by the consolidation and subdivision of codes, together with a housekeeping exercise to remove redundant records or codes. The client should be informed of the need to keep an adequate audit trail, and he may require the auditor’s assistance.

(iii) After the changeover

The auditor will need to document and assess the new system before deciding what audit approach to take. In small systems, and particularly where there are networks, there are likely to be ‘teething’ problems for the first few weeks or months after implementation.

If two systems are run in parallel, it may be possible to rely on the old system for a while.

CIS controls would you expect to find in this particular area?
GENERAL COMPUTER APPLICATION CONTROLS

General Controls: “ASDA ROME”
Relate to the entire Information System

A: Anti Virus Software: minimise the risk of loss or corruption of data

SD: System Development Controls: Use of proper programming standards, qualified programmers, testing and conversion procedures

A: Access Controls: Passwords, Locked Computer Rooms, Swipecards

ROM: Read Only Memory

E: Encryption: Help prevent hacking
Application Controls : “Abs Spec”
Relate to an individual software program

A: Authorisation Controls – Both manual & computerised to prevent the recording of invalid and inaccurate transactions

B: Batch totals

S: Screen Prompts - “Quit Yes/No” – Help prevent many types of input error

S: Sequence Checks - Ensure the completeness of input

P: Parameter (or Reasonableness) checks – is the figure for a transaction within an acceptable range e.g. customer credit limit

E: Existence Checks – ensures that the customer, supplier or employee who is being entered on a transaction file, actually exists on the master file

C: Consistency Checks – ensure that one part of the transaction being entered is consistent with another e.g. if there is a charge for carriage inwards, there should also be a charge for purchases

Note that not all computer controls are necessarily computerised!

General controls include administration controls and system development controls. Application controls are sometimes referred to as procedural controls. I have therefore provided a mnemonic which may sound ridiculous, but will help you in answering most of the computer control questions – DOFFS CASTIPOF.

{ Division of duties } G
{ }
{ Operator controls } E
{ }
{ File controls } N
{ }
{ Fire precautions and standby facilities } E
{ }
General Controls

Administration Controls

These cover the day-to-day organisation of the system environment.

(i) Division of Duties
Due to the centralised nature of processing, it is very important to ensure a full separation of staff duties within the data processing department, as can be seen from the diagram below.
However, it is also important to realise that division of duties in a computer department is not adequate for proper control. It is very important that there is a proper division and definition of duties between the computer department and the user department.

Whilst the computer department will be responsible for computer controls, such as validity checks, the user department must be responsible for controls such as authorisation of input, manual control accounts, standardised input documentation. It will be very important to ensure that areas such as error definition and error resubmission responsibilities are carefully defined.

(ii) Operator Controls

The true definition of a computer operator is someone who supervises the operation of the machine, such as loading and unloading tapes or disks, ensuring adequate paper in the printer, etc. An operator must not be confused with an input clerk. Due to the access afforded, the operator to the computer and the files, they need to be controlled very tightly, as they have a very good opportunity for deliberate destruction of data or computer fraud. Therefore the following controls should be implemented.

- At least two operators per shift to attempt to provide inter-personal supervision.
- Rotation of operator duties to avoid permanent working relationships.
- Precise operating instructions so that the operators know exactly what they are meant to be doing, and to avoid any uncertainty when action is necessary.
- Work scheduling to avoid bottlenecks.
- Regular review of computer console logs.

The computer console will record all human intervention usually by password giving the time of intervention, and the programs accessed. This log of what has been done can then be compared with the work plan of what was meant to have been done.

It is important that you try to regard controls as being preventative or detective. From the above you can see that (a) to (d) inclusive are preventative controls and (e) is purely a detective control.

(iii) File Controls

These must be broken down into two areas:

- File Storage:
  1. The establishment of a file library.
2. The recording of all files and file movement in a register.
3. The issue of files only upon written authorisation.
4. The proper labelling of all files.
5. Use of write permit tags.

File storage is important regardless of the size of the system. If we are talking about a large mainframe system, the library may be contained in a large room where many disks are stored. However, in smaller systems, the file library may be contained within a fireproof cabinet; the principles remain the same.

(b) File Reconstruction

In the event of fire, flood or any other catastrophe, it is very important that the company is able to reconstruct its records very quickly. The most common method of achieving this is three generations of file maintenance, which is sometimes known as grandfather, father, son or grandmother, mother, daughter, depending upon your preference. This is where the data from Monday is copied onto file one, the data from Tuesday is copied onto file two, the data from Wednesday is copied onto file three, the data from Thursday is copied onto file one, the data from Friday onto file two, etc. This means that, in the event of a fire during copying, the maximum data loss is only one day and the system can be reinstated from the previous day’s copy file.

A main server may be in use by the client where all terminals have access to a server. Daily backup on this type of system would be a vital control.

(iv) Fire Precautions and Standby Facilities

I do not intend to waste your time by listing out such controls as “NO SMOKING” signs. However, it is very important you understand that standby facilities will often involve reciprocal processing arrangements with other users of similar systems. The reciprocal arrangements are often very sound in theory, but in practice it is unrealistic for either party to the agreement to have adequate space capacity, at the appropriate time in the event of it being required by the other party. It is also very important to mention under this heading the need for comprehensive software and hardware maintenance contracts. This means that, in the event of any hardware or software failure in the system, the engineers can be called upon to attend the computer with only two or three hours notice.

The controls explained above relate purely to the administration of the system. As you can see, they are not particularly complicated, but their simplicity should not delude you into ignoring the area and I have included several past questions to show you examples at the end of this section.
Security:

If the client has internet/e-mail facilities available to its employees it will be of vital importance that the most up-to-date anti virus software is in use to reduce the possibility of a virus getting on the system.

The client should also encourage staff to only use the Internet and e-mail for business purposes.

System Development Controls

The controls which are about to be described are those which cover the development period from the feasibility study to the live running of the system.

Conversion Controls

These controls relate to the initial set-up of the master files during the development stage. The consistent nature of processing means that any error on the master file will cause a consistently recurring transactional error. Therefore when setting up the master file, it is very important that no errors are included from the transfer of manual standing data to computer standing data.

There are two main stages of the conversion process to which strict control should apply.

- Validity of the Data to be Converted:
  
This will mean that the data to be converted is valid. A simple example of this would be a inventory count of inventory before any computerisation of inventory records commence.

- Accuracy:

  1. Key verification, this involves the double entry of data by two different input clerks, and the software will cross check to identify any inconsistencies caused by punching errors.

  2. The checking of a printout of the entire master file to source documentation. This is obviously an incredibly long winded process and therefore only the key fields will be checked back to source documents.

Authorisation Acceptance
Because of the often long time lag between conception and implementation there can be many changes from the original specification. Therefore it is important to establish a Steering Committee or a Development Coordination Committee at the very start of the development process.

The Steering Committee should not only contain an enthusiastic ageing Chairman and Heads of Department, but should include low level users. These people will usually have a better working knowledge of the system than anybody else, and also, psychologically, it is important to ensure full commitment to the new system, which may only come if they are involved in its design.

There must also be an expert on the Steering Committee to act as a liaison between the Steering Committee and the Computer Development Department or Software House, depending upon the size of the company. The users may not be well up on modern computer lingo, and therefore the expert is there to translate their needs and demands to the system analysts, and vice versa.

Whilst the internal auditor can report into the Steering Committee, it is important that he is not actively involved in the system design. This would detrimentally affect his independence. It is not advisable for the external auditors to be involved as this can lead to a compromise in his objectivity and independence.

Every stage of the development and any changes from the original specification must be authorised in writing and included in the Steering Committee minutes.
(viii) System Documentation

This is a very important feature of systems development and it should include the following:

- Narrative description of system objectives.
- System and programme flow-charts.
- Examples of standardised input, output, documents and reports.
- Details of all system hardware, e.g. number and location of terminals.
- Organisation charts and job descriptions for all personnel involved in the system.

(ix) Testing and Training

Testing

This area can be broken down further:

Program testing:

This will involve the testing of individual programs. The main form of testing is known as Desk checking, the re-reading of coded programs by independent programmers. The testers may also run dummy data or test data through the newly written programs to ascertain whether the actual program's reaction is that which was predicted.

System testing:

The most common method is parallel running. This is where the old system is run alongside a new system. It should be performed for at least one reporting cycle, so that all possible situations can be checked. The results from the old and new systems will then be compared.

Training

The training aspect of all staff is vital for the proper running of the accounting system. This can take many forms, but must involve the tuition of small groups with hands-on experience.

Application Controls

As explained, these deal with the accuracy and completeness of input and processing, and the validity of the resulting output.

Input Controls
These will include the following:

- **Key verification:**
  
  Data is input twice by two different operators. The system will check one source against the other and bring any differences to the attention of the operators. This is an expensive edit check.

- **Format checks:**
  
  This is where the screen is designed to accept data only in pre-determined formats as shown below:

  ![Format Example]

  With this format, the input clerk can only enter an alpha code into the first field, numeric code into the second and so on. The data can only be four digits long.

- **Sequence checks:**
  
  This is fairly self explanatory. It is where the computer will check the sequence of invoice numbers or credit note numbers. If there is a break in the sequence, a warning will be given.

- **Limit or range checks:**
  
  This is one very common validation control, which has been examined in the past. The validation program includes pre-set parameters, if the data falls outside these parameters, it will be rejected or an exception report will be produced.

- **Batch control:**
  
  This is where the data is batched together and input as one. An example of a simple batch summary form is shown below:

<table>
<thead>
<tr>
<th>Account Number</th>
<th>Narrative</th>
<th>€ Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-1050</td>
<td>Ford Escort</td>
<td>11,000</td>
</tr>
<tr>
<td>16-1050</td>
<td>Golf GTi</td>
<td>13,000</td>
</tr>
<tr>
<td>16-1050</td>
<td>Astra GL</td>
<td>14,000</td>
</tr>
<tr>
<td>40-2000</td>
<td>Bloggs Garages Ltd</td>
<td>38,000</td>
</tr>
<tr>
<td>88-5150</td>
<td>Zero</td>
<td></td>
</tr>
</tbody>
</table>

© Cenit Online 2015
As you can see, the account numbers such as ledger 16 account 1050 are added to provide a hash total and the amounts are added to ensure that they equal zero. The input clerk will then enter the hash total and then enter the entire batch summary form. The validation program will check to ensure that the hash total equals the sum of the account numbers. Batching is still performed in some companies, but it is not so common as many companies rely on individual entry from remote terminals.

- **Check digit verification:**

  This is where the validity of an account number is proved by a pre-determined Algorithm. A common method is called “Modulus Eleven”. This is where the first digits of the account number are divided by 11 and the remainder should equal the last digit.

Therefore account number 20618 will be entered into the machine, the validation programme will check to ensure that the last digit is the remainder of the first three digits divided by 11. If the Algorithm is proved, the account number will be accepted as being valid.

**Processing Controls**

These controls are designed to provide reasonable assurance that computer processing has been performed as intended for the particular application. They should ensure that transaction are not lost, added to, duplicated or improperly changed; and that processing errors are identified and corrected on a timely basis.

**File Amendment Controls**

Whereas conversion controls relate to the establishment of the master file, the file amendment controls relate to the day to day changes which will always take place. They will include:

- Amendments should only be accepted by the data processing department on pre-printed, pre-numbered master file amendment forms duly authorised.

- When the amendment has been initiated, a printout of the amendment will be sent to the originator of the amendment for checking.

- The originator will then check the printout and evidence the check by signature.

- The printout will then be returned to the DP department and the amendments finalised.

The above controls are amendment controls at their strictest and are probably only suitable for a payroll department. If you get a question on this area in the exam, please try to remember to adopt the controls I have given you, to the situation given. If, for example, you are asked about the file amendment controls for a fixed asset register, it would not need to be as strict as the ones described above.
At the end of each month, a summary of all master file amendments will be sent to the Heads of department.

**Audit Software**

Be careful with questions which ask for a discussion on the software which can be used during the course of an audit, remember the easy ones first

**WORD:** The Bank confirmation letter will be copied from last year with date changes.

The Receivables Circularisation will be prepared as a mail merge using a standard letter on file.

**EXCEL:** The budget will be prepared on a spread sheet. Analytical review can be conducted in excel.

Sampling: Programmes will be used to generate random numbers and also in the use of Monetary Unit Sampling (MUS).

**Maintaining Master Files**

Master files are of particular significance as any inaccuracy in these will result in error(s) which will be repeated. Important controls would include:

- A rigorous system in place to ensure that Master files can be reconstructed in the event of a system crash
- Copies of all master files to be held in a secure location outside the computer room
- **Master files to be updated by persons not connected with the execution or processing of transactions**
- Careful validation of input data to the master file to prevent corruption
- One to one checking of all input data
How do auditors use computers in performing audits?

The following areas have been suggested as suitable applications of PC’s to audit work:

(a) Spreadsheets

Spreadsheets are ‘sheets’, similar to analysis paper, divided into individually referenced ‘cells’ that can be programmed with formulae in order to calculate and recalculate quickly and accurately. They hold much more data than can be comfortably held on analysis paper.

Spreadsheets can be used in the following areas:

(i) Accounts preparation

Good quality inexpensive, standardised accounts preparation packages are now available and are suitable for anything from the smallest of entities, to large consolidation packages. Many of these are spreadsheet based.

(ii) Time/cost budgeting

The firm’s staffing requirements and planning can be performed using spreadsheets and individual audits can be costed and budgeted using integrated software.

(iii) Analytical procedures

Analytical procedures that involve the calculation of trends, ratios and other relationships can be dealt with effectively using spreadsheets. Data in relation to financial performance and position can be held for comparison with subsequent years, and the use of spreadsheets facilitates consistency, particularly where there are changes of staff.
(b) Statistical packages

This type of package is particularly useful in the application of sampling procedures.

Packages can, for example:

(i) select the number of items to test, within given parameters of risk and assurance required;
(ii) select which items to test, at random, on a systematic, block or monetary basis;
(iii) analyse results, by means of extrapolation to the population as a whole.

Such packages increase the efficiency of the audit as they promote accuracy and speed, and facilitate delegation and review. The danger is that the package will be used mechanically, without the proper use of professional judgement and that the results will be assumed to be correct, simply because they have been produced by the computer.

If the auditor’s PCs can be connected to the client’s PCs, or are compatible with them, there will be no need to input data relating to populations from which samples are drawn, as they can be taken directly from the client’s system. This may represent a considerable time and cost saving.

(c) Word processing

Word processing is used in almost all areas of the audit. It is used for the routine production of reports, faxes, letters, memos, emails and other communications.

It reduces the need for support staff and shortens the time in which documents can be produced, as the packages are user-friendly and can be used by professional staff. It also improves client and staff relations, particularly where email can be used to eliminate the physical movement of large documents that need to be reviewed or edited.

Specifically, it can be used to produce audit programs, audit planning documentation, ordinary working papers, lead schedules, and almost all other current file documentation.

Providing there is adequate backup and proper contingency planning, it may be possible to reduce the number of paper based files kept, with a consequent reduction in storage costs.
Use of CAATS (Computer Assisted Audit Techniques) in Auditing

CAATS are now available as standardised packages, but are generally still only used for larger clients as they are relatively expensive. They are, however, cost effective in the long run as they are quicker and more accurate than conventional techniques. The effective use of CAATS relies on the cooperation of clients and a proper understanding of their use.

There are two basic categories of CAAT:

(i) Audit Software

N.B. Audit software is primarily used for substantive procedures. Client data is processed though the auditor’s programs. These programs can, for example:

1 check additions (recast!);

2 select high value, static, or negative transactions and balances, for review;

3 perform, or re-perform the ageing of a ledger;

4 select samples for further testing.
The data can be downloaded directly from the client’s system, or re-input into the auditor’s system. Obviously, the better the communications between auditor and client systems, the more efficient this process will be.

‘Embedded audit facilities’ amount to audit software that has been written into the client’s system, to trap items as they are processed for further testing at a later date.

(ii) Test data
Test data is auditor generated data (very reliable) that is used primarily for testing controls. The auditor will test access controls over the system by attempting to gain unauthorised entry into it, or by attempting to process invalid data. For example, unauthorised passwords, employee names or numbers may be used in an attempt to gain entry. Incomplete transactions, transactions with incorrect coding, transactions outside programmed parameters, and transactions with non-existent customers or suppliers - all of these may be used in testing to ensure that the system properly rejects invalid transactions.

Test data carries with it the inherent risk of corruption of client data.

‘Integrated test facilities’, which give the auditor his own section of the general ledger avoid this, and permit the testing of longer-term controls.

Audit Practice considerations in Using CAAT’s
The costs of investing in PCs, the associated software, refurbishment, training and maintenance must be balanced against the benefits of a more streamlined and efficient audit practice.

Precautions

• Client’s files must not be corrupted or damaged.
• Files used for testing must be complete, accurate and identical to, if not the same as, files currently used by the client. (i.e. a representative sample)

• Computer audit programs must be amended to account for developments in the client’s applications.

Considerations Affecting Use of CAATS

- Computer knowledge of the audit team
- Cost/benefit analysis
- Time available
- Availability/compatibility of client computer systems
- System features such as lack of visible audit/transaction trail
- Potential for corruption of client data and difficulties in removing test data from client system

Auditing Around the Computer

“Auditing Around the Computer” = This term means that audit activity is focused primarily on ensuring that the source documentation is processed correctly and the auditor verifies this by checking the source documentation to the output documentation. The “internal” software of the computer is not documented or audited by the auditor.

This method of auditing increases audit risk because:

- The actual computer files and programs are not tested; the auditor has no auditor generated evidence that the programs are working as documented
- Where errors are found in reconciling inputs to outputs, it may be difficult or even impossible to determine why those errors occurred. Useful amendments to clients systems (Communication of Audit to Those Charged With Governance ISA 260) cannot be made and there is an increased possibility of audit report modifications
Auditors’ Use of Computers

Assist Auditors’ Work
- Where Used
  - Flowcharts
  - Risk Assessment
  - Audit Programs
  - Analytical Procedures
  - Working Papers

- Concerns
  - Back-up
  - Security Physical/Virus
  - Adequacy of Docs

Gather Audit Evidence
- Types
  - Audit Software
  - Test Data
  - Embedded Software
  - Parallel Simulation

- Concerns
  - Cost
  - Effect on Clients System
  - Dummy Data
SAMPLE QUESTION AND ANSWER - CAATs (Audit Software)

You are an audit senior with an interest in computer auditing and you are employed in a firm of Accountants. You have just been assigned to assist in the audit of a new client of your firm, TECHNO Ltd. (“TECHNO”), a software development company, whose parent company is an internationally known company based in Frankfurt.

The main expense of the company is Wages and Salaries. TECHNO employs in excess of 5,000 staff, a small percentage of whom are employed in administrative and management functions. The company operates a highly computerised recording and accounting system. For the past 10 years the company has operated a computer-based accounting system developed in-house. It is currently in the process of developing a new system, the implementation of which is planned for the month following the audit.

The audit manager is concerned about the efficiency and effectiveness of the audit, especially given the large number of employees on a weekly salary and the extent of computerisation of the client’s processes. Also, there is a shortage of audit assistants to carry out the detailed tests at the time the audit is to be carried out. The deadline for completion of the audit fieldwork is fixed so that TECHNO’s results can be included in the financial statements of the German parent.

The audit manager has read that Computer Assisted Audit Techniques (CAATs) would afford opportunities to assist in the performance of the audit work. However, he is relying on you as neither he nor any other manager within the firm has had any practical experience of using CAATs. There is a budget available for the purchase of whatever additional computer equipment or programs you require. He has asked you to brief him on the audit and on the potential use of CAATs.

Requirement

Respond to the audit manager by drafting a file note to include, in particular, each of the following:

(a) Assuming that CAATs can be used, your advice (together with reasoning) as to the choice of a systems based approach or a wholly substantive audit approach to Wages and Salaries.

6 Marks

(b) Eight specific examples, in bullet point format, of how CAATs could be used to obtain audit evidence on TECHNO’s Wages and Salaries figure.

8 Marks

(c) An outline of the main steps in designing and running CAATs on TECHNO’s Wages and Salaries figure.

6 Marks

Total 20 Marks

SOLUTION

© Cenit Online 2015
In the circumstances of “TECHNO”, as described in the background information, a wholly substantive audit approach is considered more appropriate. A systems based audit approach would be inappropriate to test the operation of the enterprise’s computer systems for the following reasons:

(i) The relatively high degree of development time involved in setting up such tests.

(ii) Testing the internal control system for one year only as the company is in the process of developing a new system, the implementation of which is planned for the month following the audit.

CAATs can be used as part of the substantive audit work and can give extensive audit coverage, rather than a small sample (for systems testing purposes) dealing with a large volume of transactions. The use of test data is ruled out in these circumstances because of the risk that test data will corrupt company files unless appropriate corrective action is taken. This would be considered high risk in these circumstances because of the low level of expertise existing within the audit firm. The background information indicates that neither the audit manager nor any other senior party within the firm has any practical experience of the use of CAATs.

(B)

It is suggested that CAATs could be used to obtain audit evidence on TECHNO’s wages and salaries figure as follows:

Use of exception reports to check:

- Changes to standing data
- Salaries >€ X
- Duplicate employees (sequence checking)
- Duplicate PPS numbers
- Employees without PPS number

Detecting unreasonable items, for example hours worked < 20 or >60 per week.

Analysis and pattern detection:

- Detecting violations of systems rules by aging, sorting, summarising.
- Compare average salary for different departments.
- Compare overtime payments between different teams.

Enable the performing of statistical analyses such as generating frequency distributions, calculating the mean and standard deviation.
Verify control totals

- Check PAYE, PRSI calculations.
- Recalculate overtime/bonus payments.
- Check the value of items on a file to ensure they agree with control totals.

Validate date

- Check that all employees have a valid joining date.

Selection of items for audit testing

- Joiners and leavers.
- Sample selection/stratification.

Completeness checks

- Are all employee or department numbers included in all weeks of the year.

Amendments to standing data.

(c) In designing and running CAATs on TECHNO’s wages and salaries figure, the standard principle of Planning, Controlling and Recording apply. The following main steps are suggested:

- Decide on the specific audit objectives.
- Determine the content and accessibility of client’s computer files (or client systems).
- Decide on what procedures are to be performed on the data.
- Define the output requirements.
- Identify the audit and client personnel who need to be involved and that their level of skill/expertise within the firm is appropriate.
- Execute CAAT.
- Evaluate the results.
- Document each step as it occurs and this documentation should allow performance of the CAAT if required.

- Define audit software to be used.