AUDITING IN A COMPUTER-BASED

RELEVANT TO CAT PAPER 8 AND ACCA QUALIFICATION PAPERS F8

The accounting systems of many companies, large and small, are computer-based; questions in all ACCA audit papers reflect this situation.

Students need to ensure they have a complete understanding of the controls in a computer-based environment, how these impact on the auditor's assessment of risk, and the subsequent audit procedures. These procedures will often involve the use of computer-assisted audit techniques (CAATs).

The aim of this article is to help students improve their understanding of this topic by giving practical illustrations of computer-based controls and computer-assisted techniques and the way they may feature in exam questions.

THE AIM OF THIS ARTICLE IS TO HELP STUDENTS IMPROVE THEIR UNDERSTANDING OF THIS TOPIC BY GIVING PRACTICAL DEMONSTRATIONS OF COMPUTER-BASED CONTROLS AND TECHNIQUES, AND THE WAYS THEY MAY FEATURE IN EXAMS.

Relevant auditing standards

References will be made throughout this article to the most recent guidance in standards:

- ISA 300 (Redrafted) *Planning an Audit of Financial Statements*
- ISA 315 (Redrafted) *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment*
- ISA 330 (Redrafted) *The Auditor's Responses to Assessed Risks.*

Internal controls in a computer environment

The two main categories are *application controls* and *general controls.*

Application controls

These are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications. Application controls can be preventative or detective in nature and are designed to ensure the integrity of the accounting records.

Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data. These controls help ensure that transactions occurred, are authorised and are completely and accurately recorded and processed (ISA 315 (Redrafted)).

Application controls apply to data processing tasks such as sales, purchases and wages procedures and are normally divided into the following categories:

(i) Input controls

Examples include batch control totals and document counts, as well as manual scrutiny of documents to ensure they have been authorised. An example of the operation of batch controls using accounting software would be the checking of a manually produced figure for the total gross value of purchase invoices against that produced on screen when the batch-processing option is used to input the invoices. This total could also be printed out to confirm the totals agree.

The most common example of programmed controls over the accuracy and completeness of input are edit (data validation) checks when the software checks that data fields included on transactions by performing:

- reasonableness check, eg net wage to gross wage
- existence check, eg that a supplier account exists
- character check, eg that there are no alphabetical characters in a sales invoice number field
- range check, eg no employee's weekly wage is more than $2,000
- check digit, eg an extra character added to the account reference field on a purchase invoice to detect mistakes such as transposition errors during input.

Studying Papers F8 or P7?
Performance Objectives 17 and 18 are linked

ENVIRONMENT

AND P7 (INT AND UK)

When data is input via a keyboard, the software will often display a screen message if any of the above checks reveal an anomaly, eg 'Supplier account number does not exist'.

(ii) Processing controls

An example of a programmed control over processing is a run-to-run control. The totals from one processing run, plus the input totals from the second processing, should equal the result from the second processing run. For instance, the beginning balances on the receivables ledger plus the sales invoices (processing run 1) less the cheques received (processing run 2) should equal the closing balances on the receivable ledger.

(iii) Output controls

Batch processing matches input to output, and is therefore also a control over processing and output. Other examples of output controls include the controlled resubmission of rejected transactions, or the review of exception reports (eg the wages exception report showing employees being paid more than $1,000).

(iv) Master files and standing data controls

Examples include one-for-one checking of changes to master files, eg customer price changes are checked to an authorised list. A regular printout of master files such as the wages master file could be forwarded monthly to the personnel department to ensure employees listed have personnel records.

General controls

These are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, mini-frame and end-user environments. General IT controls that maintain the integrity of information and security of data commonly include controls over the following:

- data centre and network operations
- system software acquisition, change and maintenance
- program change
- access security
- application system acquisition, development, and maintenance (ISA 315 (Redrafted))

'End-user environment' refers to the situation in which the users of the computer systems are involved in all stages of the development of the system.

(i) Administrative controls

Controls over 'data centre and network operations' and 'access security' include those that:

- prevent or detect errors during program execution, eg procedure manuals, job scheduling, training and supervision; all these prevent errors such as using wrong data files or wrong versions of production programs
- prevent unauthorised amendments to data files, eg authorisation of jobs prior to processing, back up and physical protection of files and access controls such as passwords
- ensure the continuity of operations, eg testing of back-up procedures, protection against fire and floods.

(ii) System development controls

The other general controls referred to in ISA 315 cover the areas of system software acquisition development and maintenance; program change; and application system acquisition, development and maintenance.

'System software' refers to the operating system, database management systems and other software that increases the efficiency of processing. Application software refers to particular applications such as sales or wages. The controls over the development and maintenance of both types of software are similar and include:

STUDENTS NEED TO ENSURE THEY HAVE A COMPLETE UNDERSTANDING OF THE CONTROLS IN A COMPUTER-BASED ENVIRONMENT, HOW THESE IMPACT ON THE AUDITOR'S ASSESSMENT OF RISK, AND THE RESULTING AUDIT PROCEDURES.

- Controls over application development, such as good standards over the system design and program writing, good documentation, testing procedures (eg use of test data to identify program code errors, pilot running and parallel running of old and new systems), as well as segregation of duties so that operators are not involved in program development
- Controls over program changes – to ensure no unauthorised amendments and that changes are adequately tested, eg password protection of programs, comparison of production programs to controlled copies and approval of changes by users
- Controls over installation and maintenance of system software – many of the controls mentioned above are relevant, eg authorisation of changes, good documentation, access controls and segregation of duties.

Exam focus
Students often confuse application controls and general controls. In the June 2008 CAT Paper 8 exam, Question 2 asked candidates to provide examples of application controls over the input and processing of data. Many answers referred to passwords and physical access controls – which are examples of general controls – and thus failed to gain marks.

STUDENTS OFTEN CONFUSE APPLICATION CONTROLS AND GENERAL CONTROLS. IN THE JUNE 2008 CAT PAPER 8 EXAM, QUESTION 2 ASKED CANDIDATES TO PROVIDE EXAMPLES OF APPLICATION CONTROLS OVER THE INPUT AND PROCESSING OF DATA. MANY ANSWERS REFERRED TO EXAMPLES OF GENERAL CONTROLS – AND THUS FAILED TO GAIN MARKS.

Computer-assisted audit techniques

Computer-assisted audit techniques (CAATs) are those featuring the 'application of auditing procedures using the computer as an audit tool' (*Glossary of Terms*). CAATs are normally placed in three main categories:

(i) Audit software
Computer programs used by the auditor to interrogate a client's computer files; used mainly for substantive testing. They can be further categorised into:

- *Package programs (generalised audit software)* – pre-prepared programs for which the auditor will specify detailed requirements; written to be used on different types of computer systems
- *Purpose-written programs* – perform specific functions of the auditor's choosing; the auditor may have no option but to have this software developed, since package programs cannot be adapted to the client's system (however, this can be costly)
- *Enquiry programs* – those that are part of the client's system, often used to sort and print data, and which can be adapted for audit purposes, eg accounting software may have search facilities on some modules, that could be used for audit purposes to search for all customers with credit balances (on the customers' module) or all inventory items exceeding a specified value (on the inventory module).

Using audit software, the auditor can scrutinise large volumes of data and present results that can then be investigated further. The software consists of program logic needed to perform most of the functions required by the auditor, such as:

- select a sample
- report exceptional items
- compare files
- analyse, summarise and stratify data.

The auditor needs to determine which of these functions they wish to use, and the selection criteria.

Exam focus
Sometimes, questions will present students with a scenario and ask how CAATs might be employed by the auditor. Question 4 in the December 2007 Paper F8 exam required students to explain how audit software could be used to audit receivables balances. To answer this type of question, you need to link the functions listed above to the normal audit work on receivables. Students should refer to the model answer to this question.

The following is an example of how this could be applied to the audit of wages:

- Select a random sample of employees from the payroll master file; the auditor could then trace the sample back to contracts of employment in the HR department to confirm existence

QUESTIONS MAY PRESENT STUDENTS WITH A SCENARIO AND ASK HOW CAATs MIGHT BE EMPLOYED BY THE AUDITOR. QUESTION 4 IN THE DECEMBER 2007 F8 EXAM REQUIRED STUDENTS TO EXPLAIN HOW AUDIT SOFTWARE COULD BE USED TO AUDIT RECEIVABLES BALANCES. TO ANSWER, YOU NEED TO LINK THE FUNCTIONS TO AUDIT WORK ON RECEIVABLES.

- Report all employees earning more than $1,000 per week
- Compare the wages master file at the start and end of the year to identify starters and leavers during the year; the auditor would then trace the items identified back to evidence, such as starters' and leavers' forms (in the HR department) to ensure they were valid employees and had been added or deleted from the payroll at the appropriate time (the auditor would need to request that the client retain a copy of the master file at the start of the year to perform this test)
- Check that the total of gross wages minus deductions equates to net pay.

(ii) Test data

Test data consists of data submitted by the auditor for processing by the client's computer system. The principle objective is to test the operation of application controls. For this reason, the auditor will arrange for dummy data to be processed that includes many error conditions, to ensure that the client's application controls can identify particular problems.

Examples of errors that might be included:

- supplier account codes that do not exist
- employees earning in excess of a certain limit
- sales invoices that contain addition errors
- submitting data with incorrect batch control totals.

Data without errors will also be included to ensure 'correct' transactions are processed properly.

Test data can be used 'live', ie during the client's normal production run. The obvious disadvantage with this choice is the danger of corrupting the client's master files. To avoid this, an integrated test facility will be used (see other techniques below). The alternative (dead test data) is to perform a special run outside normal processing, using copies of the client's master files. In this case, the danger of corrupting the client's files is avoided – but there is less assurance that the normal production programs have been used.

(iii) Other techniques

There are increasing numbers of other techniques that can be used; the main two are:

- *Integrated test facility* – used when test data is run live; involves the establishment of dummy records, such as departments or customer accounts to which the dummy data can be processed. They can then be ignored when client records are printed out, and reversed out later.
- *Embedded audit facilities (embedded audit monitor)* – also known as resident audit software; requires the auditor's own program code to be embedded into the client's application software. The embedded code is designed to perform audit functions and can be switched on at selected times or activated each time the application program is used. Embedded facilities can be used to:
  - Gather and store information relating to transactions at the time of processing for subsequent audit review; the selected transactions are written to audit files for subsequent examination, often called system control and review file (SCARF)
  - Spot and record (for subsequent audit attention) any items that are unusual; the transactions are marked by the audit code when selection conditions (specified by the auditor) are satisfied. This technique is also referred to as tagging.

The attraction of embedded audit facilities is obvious, as it equates to having a perpetual audit of transactions. However, the set-up is costly and may require the auditor to have an input at the system development stage. Embedded audit facilities are often used in real time and database environments.

Impact of computer-based systems on the audit approach

The fact that systems are computer-based does not alter the key stages of the audit process; this explains why references to the audit of computer-based systems have been subsumed into ISAs 300, 315 and 330.

(i) Planning

The Appendix to ISA 300 (Redrafted) states 'the effect of information technology on the audit procedures, including the availability of data and the expected use of computer-assisted audit techniques' as one of the characteristics of the audit that needs to be considered in developing the overall audit strategy.

(ii) Risk assessment

'The auditor shall obtain an understanding of the internal control relevant to the audit.' (ISA 315 (Redrafted))

The application notes to ISA 315 identify the information system as one of the five components of internal control. It requires the auditor to obtain an understanding of the information system, including the procedures within both IT and manual systems. In other words, if the auditor relies on internal control in assessing risk at an assertion level, s/he needs to understand and test the controls, whether they are manual or automated. Auditors often use internal control evaluation (ICE) questions to identify strengths and weaknesses in internal control. These questions remain the same – but in answering them, the auditor considers both manual and automated controls.

For instance, when answering the ICE question, 'Can liabilities be incurred but not recorded?', the auditor needs to consider manual controls, such as matching goods received notes to purchase invoices – but will also consider application controls, such as programmed sequence checks on purchase invoices. The operation of batch control totals, whether programmed or performed manually, would also be relevant to this question.

(iii) Testing

'The auditor shall design and perform further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level.' (ISA 330 (Redrafted))

This statement holds true irrespective of the accounting system, and the auditor will design compliance and substantive tests that reflect the strengths and weaknesses of the system. When testing a computer information system, the auditor is likely to use a mix of manual and computer-assisted audit tests.

'Round the machine (computer)' v 'through the machine (computer)' approaches to testing

Many students will have no experience of the use of CAATs, as auditors of clients using small computer systems will often audit 'round the machine'. This means that the auditor reconciles input to output and hopes that the processing of transactions was error-free. The reason for the popularity of this approach used to be the lack of audit software that was suitable for use on smaller computers. However, this is no longer true, and audit software is available that enables the auditor to interrogate copies of client files that have been downloaded on to a PC or laptop. However, cost considerations still appear to be a stumbling block.

In the 'through the machine' approach, the auditor uses CAATs to ensure that computer-based application controls are operating satisfactorily.

THE KEY OBJECTIVES OF AN AUDIT DO NOT CHANGE IN A COMPUTER ENVIRONMENT. THE AUDITOR STILL NEEDS TO OBTAIN AN UNDERSTANDING OF THE SYSTEM IN ORDER TO ASSESS CONTROL RISK AND PLAN AUDIT WORK TO MINIMISE DETECTION RISK. THE LEVEL OF AUDIT TESTING WILL DEPEND ON THE ASSESSMENT OF KEY CONTROLS.

Conclusion

The key objectives of an audit do not change in a computer environment. The auditor still needs to obtain an understanding of the system in order to assess control risk and plan audit work to minimise detection risk. The level of audit testing will depend on the assessment of key controls. If these are programmed controls, the auditor will need to 'audit through the computer' and use CAATs to ensure controls are operating effectively.

In small computer-based systems, 'auditing round the computer' may suffice if sufficient audit evidence can be obtained by testing input and output.

Peter Byrne is assessor for CAT Paper 8