Controlling & Auditing Information System

IT Controls

Prepared by:

Basuki Rahmad, Dr, CISA, CISM

2011

Table of Contents

1 Introduction and module contents 3

2 IT and the Audit Process 5

3 The IT controls model 7

4 Planning an IT controls review 14

5 Documenting IT systems 16

6 Organisation and management controls 28

7 IT Operations 42

8 Physical and environmental controls 47

9 Logical access controls 54

10 Change management 68

11 Network controls and use of the Internet 78

12 Third party service providers 79

13 End user computing controls 88

14 Introduction to application controls 95

15 Application security 101

16 Input, processing and output controls 105

17 Masterfile and standing data controls 128

1 Introduction and module contents

1.1 Module objectives

The main aim of this module is to teach the IT audit trainees how to carry out a review of a client's IT system and the applications which are associated with the processing or reporting of financial and operations transactions. These notes include detailed coverage of controls at the management, installation and application levels, together with the identification and testing of key controls.

To satisfy the main objective, this IT controls module aims to:

- identify and document key business systems;
- undertake a review of the client's computerised controls, including management controls, operational controls and application controls;
- test key IT controls;
- determine the effect of IT systems on the audit process and understand the impact of IT control weaknesses on the audit approach;
- make recommendations for improving the client's internal controls; and
- understand the client's need for business recovery planning .

Many of the control concepts identified in these notes are applicable to the control of both financial and non-financial systems. Depending on the scope of an audit and each SAI's mandate, the IT auditor may be required to review the security and controls in financial and non-financial systems.

NOTE : Business continuity planning is a large subject in itself and consequently the related student guidance are contained within a separate set of notes.

Trainees should be aware that the IT audit standards and working practices are likely to differ from one SAI to the other. The approach suggested within this module should be adapted to meet local standards and needs. The standards and guidelines issued by several international and national bodies as detailed in the module on 'Introduction to IT Audit' should also be kept in view while carrying out a review of the controls.

The subjects covered in this module are as follows:

- IT and the Audit Process;
- IT Controls model;
- Planning a controls review;
- Documenting IT systems;

- Organisation and management controls;
- IT operations;
- Physical and environmental controls;
- Logical access controls;
- Change management;
- Network controls and use of the Internet;
- Third party service providers;
- End user computing controls;
- Introduction to application controls;
- Application security;
- Input, process and output controls; and
- Masterfile and standing data controls.

2 IT and the Audit Process

2.1 Change in the type and nature of internal controls

The internal controls within a client's IT systems, both manual and computerised, can be divided into several categories.

- **Personnel** : Whether or not staff are trustworthy, if they know what they are doing and, if they have the appropriate skills and training to carry out their jobs to a competent standard.

- **Segregation of duties** : a key control in any system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction from start to finish. Various stages in the transaction cycle are spread between two or more individuals.

- **Authorisation procedures**: to ensure that transactions are approved. In some on-line transaction systems written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).

- **Record keeping**: the controls over protection and storage of documents, transaction details, audit trails etc.

- **Access to assets and records**: In the past manual systems could be protected from unauthorised access through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's data and computer programs are vulnerable to unauthorised amendment at the computer or from remote locations. The use of wide area networks, including the Internet, has increased the risk of unauthorised access. The nature and types of controls available have changed to address these new risks.

- **Management supervision and review**: Management's supervision and review helps to deter and detect both errors and fraud.

The important issue to consider for an auditor is how these basic types of control differ in a computerised environment. For example:

Segregation of duties : segregation of duties in a computerised system is different from segregation of duties in a manual system. For instance, in the manual accounting system, the auditor was primarily concerned with segregation of duties in the finance department. However, in a computerised system, the auditor should **also** be concerned with the segregation of duties within the IT department.

Within an IT environment, the staff in the computer department may be the only client staff with a detailed knowledge of the interrelationship between the source of data, how it is

processed and distribution and use of output. It is possible that the client's IT personnel will be aware of any control weaknesses which exist. IT staff may also be in a position to alter transaction data or even the financial applications which process the transactions. In such a situation, all they would require is a motive.

Concentration of programs and data : Transactions and masterfile data (e.g. pay rates, approved suppliers lists etc.) may be stored in a computer readable form on one IT system or on a number of distributed installations. Computer programs such as file editors are likely to be stored in the same location as the data. Therefore, in the absence of appropriate controls over these programs and utilities, there is an increased risk of unauthorised access to, and alteration of key data.

Without adequate controls anyone could look at the records and make amendments, some of which could remain undetected.

2.2 New causes and sources of error

System generated transactions

IT systems may have the ability to initiate, approve and record transactions. This is likely to become increasingly common as more organisations begin to install expert systems and electronic data interchange (EDI) trading systems. The main reason clients are starting to use these types of system is because they can increase processing efficiency (for example, if a computer system can generate transactions automatically there will be no need to employ someone to do it manually, and hence lower staff costs).

Automated transaction processing systems can cause the auditor problems. For example when gaining assurance that a transaction was properly authorised or in accordance with delegated authorities, the auditor may need to look at the application's programming to determine if the programmed levels of authority are appropriate.

Automated transaction generation systems are frequently used in 'just in time' (JIT) inventory and stock control systems: When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier (perhaps using EDI technology).

Systematic Error

Computers are designed to carry out processing on a consistent basis. Given the same inputs and programming, they invariably produce the same output. This consistency can be viewed in both a positive and a negative manner.

If the computer is doing the right thing, then with all other things being equal, it will continue to do the right thing every time. Similarly, if the computer is doing the wrong thing and processing a type of transaction incorrectly, it will continue to handle the same type of transactions incorrectly every time. Therefore, whenever an auditor finds an error in a computer processed transaction, s(he) should be thorough in determining the underlying reason for the error. If the error is due to a systematic problem, the computer may have processed hundreds or thousands of similar transactions incorrectly.

3 The IT controls model

3.1 The overall internal controls framework

3.1.1 Introduction

When reviewing a client's control systems, the auditor will be able to identify three components of internal control. Each component is aimed at achieving different objectives. The financial auditor will be most familiar with:

- Accounting controls, i.e. those controls which are intended to safeguard the client's assets and ensure the reliability of the financial records;

The other two types of control likely to be encountered are:

- Operational controls: these deal with the day to day operations , functions and activities to ensure that the operational activities are contributing to business objectives;

- Administrative controls : these are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

3.1.2 Auditor's categorisation of controls

As mentioned in the introductory module, we categorise the controls as being either:

Preventive controls: These controls are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system.

Detective controls: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a the use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend.

Corrective controls : Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control.

3.1.3 Elements of internal control

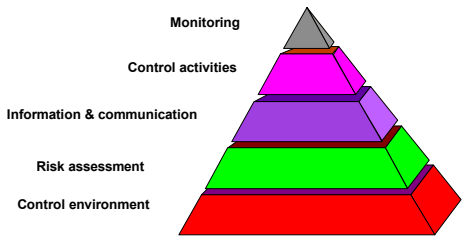
There are five elements which contribute to a client's internal control structure. These are as follows:

- The general controls environment : This includes the factors which set the tone of the business and the working environment. Controls within this level are normally

associated with high level policies, ethical values, the business culture and the human resources structure.

- Risk assessment : The assessment of risks is usually seen as a first proactive step in the control process. When designing specific detailed controls you should have an idea of what the control is supposed to do. This should include an assessment of the threats, vulnerabilities and impact. If there is no risk then there is little point is spending time and effort putting in a control. (Risk assessment is covered in greater depth in the IT security module).
- Information and communications : These consist of controls which enable staff to receive and control information within the business.
- Control activities : these are controls which ensure that the business continues to operate in the manner expected by senior management.
- Monitoring: there should be some form of monitoring to ensure that the policies and procedures continue to function and remain appropriate.

Within the client's IT environment there are IT related controls within each of these categories.



Within the client's financial control environment, all the levels of control identified aim to ensure that:

- assets are safeguarded;
- transactions are accurately recorded;
- all valid transactions have been recorded in a timely manner;
- all transactions were authorised; and
- all transactions were processed correctly and in accordance with management's requirements.

3.1.4 Limitations of internal controls

To be effective, internal control systems must be well designed and operate as intended.

However, there are some inherent limitations to any system of internal control.

- Assurance provided by controls is reasonable, rather than absolute. The cost of gaining absolute assurance would be prohibitive.
- There is a risk that controls may become inadequate. For example, changes in a system may reduce the effectiveness of a control.
- The effectiveness of controls may depend on the client staff responsible for ensuring the controls are operating. To a certain extent the successful operation of internal controls relies upon the honesty and pride and sense of duty that people have when fulfilling their duties. These assumptions about employee behaviour add to the limitations of internal control. People are not predicable like computers. Basic assumptions may include :

  - prompt disciplinary action will deter individuals from fraud;
  - people report irregularities;
  - personal relationships within the organisation will not influence the "formal" relationships established by the organisation;
  - people will perform only those functions required by the organisational structure;
  - the existence of documentary evidence for an action implies that the action has taken place. In other words, employees will not initial a document as evidence of their review, if they have not reviewed it; and
  - employees have sufficient training, experience, time and motivation to do their duties conscientiously.

Controls designed to ensure the execution and recording of transactions will be ineffective against irregularities resulting from management's decision to occasionally by-pass controls. Because of these inherent limitations of internal control, an auditor cannot use tests of controls alone to obtain audit evidence in accordance with generally accepted auditing standards.

When an auditor chooses to rely on internal control to reduce substantive tests, the audit approach is said to be "system" based or controls reliant.

3.2 General and application controls

Within the IT environment two levels of control can be identified:

- General IT controls and
- Application controls.

At the lowest level, there are general controls, which are concerned with the general environment in which the IT systems are developed, operated, managed and maintained. General IT controls establish a framework of overall control for the IT activities and provide some assurance that the overall control objectives are satisfied. In essence they act as a foundation, onto which specific application controls can be designed.

The other level of control consists of application controls. These are specific control procedures over the applications which can provide assurance that all transactions are authorised and recorded, processed completely, accurately and on a timely basis. Application controls may consist of manual procedures carried out by users (user controls) and automated procedures or controls performed by the computer software.

3.2.1 General IT controls

General IT controls are concerned with the client's IT infrastructure, including any IT related policies, procedures and working practices. They are not specific to individual transaction streams or particular accounting packages or financial applications. In most instances the general controls elements of an IT review will concentrate on the client's IT department or similar function. Components of general controls include:

- organisation and management (IT policies and standards) controls;
- segregation of duties;
- physical controls (access and environment);
- logical access controls;
- system development and program change controls;
- controls over computer personnel (including programmers, system analysts, and computer operations staff). Note : this can cover both internal and external IT services;
- controls to ensure that the computer systems are there and working when they are needed, i.e. business continuity planning; and
- controls over end user computing.

3.2.2 Application controls

Application controls are particular to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance (primarily to management) that all transactions are valid, authorised and recorded.

Since application controls are closely related to individual transactions it is easier to see why testing the controls will provide the auditor with audit assurance as to the accuracy of a particular account balance. For example, testing the controls in a payroll application would provide assurance as to the payroll figure in a client's accounts. It would not be obvious that testing the client's general IT controls (e.g. change control procedures) would provide a similar level of assurance for the same account balance.

As they are related to transaction streams application controls normally include:

- controls over the input of transactions;
- controls over processing;
- controls over output; and
- controls over standing data and masterfiles.

Many application controls are simply computerised versions of manual controls, e.g. computerised authorisation by a supervisor using an access code rather that putting a signature on a piece of paper.

3.3 Relationship between general controls and application

controls

One way of looking at the relationship between general and application controls is to allocate the general controls to protecting the applications and the transaction databases. General controls provide the applications with the resources they need to operate and ensure that unauthorised changes cannot be made to either the applications (i.e. they protected from reprogramming) or the underlying databases (the large collection of transaction data).

Meanwhile, the application controls operate on individual transactions and ensure that they are correctly input, processed and output.

3.3.1 The IT controls "onion"

In this model we start in the middle of the onion with the financial statements and work our way out through successive layers of control. These layers, when put together should reduce the risk that the financial statements will contain material errors when we, as financial auditors, start auditing them.

Note: this chapter is only intended to give the students a visual interpretation of the layers of control using a financial accounting system. The controls will be covered in depth in later chapters.

- The financial statements: the eventual goal, where the transactions are eventually summarised and printed out. Possible issues or risks the auditor should consider include:

  - are the accounts complete, i.e. does it include our payment?

  - has the payment been correctly disclosed as a payment, or have the charts of account or summarisation rule been amended.

- Output controls: Whilst the payment (cheques or EFT payments file) was in the spooler awaiting printing or transmission can we be sure that the details have not been altered and the payment redirected to an off-shore bank account.

- Processing controls: Has the payment been correctly processed using the correct labour rates or overhead charges?

- Input controls: Errors may have arisen when the transaction was being entered, for example transposition errors. The transaction may be fraudulent or unauthorised. The input clerk may have entered the wrong date putting the transaction in the wrong accounting period.

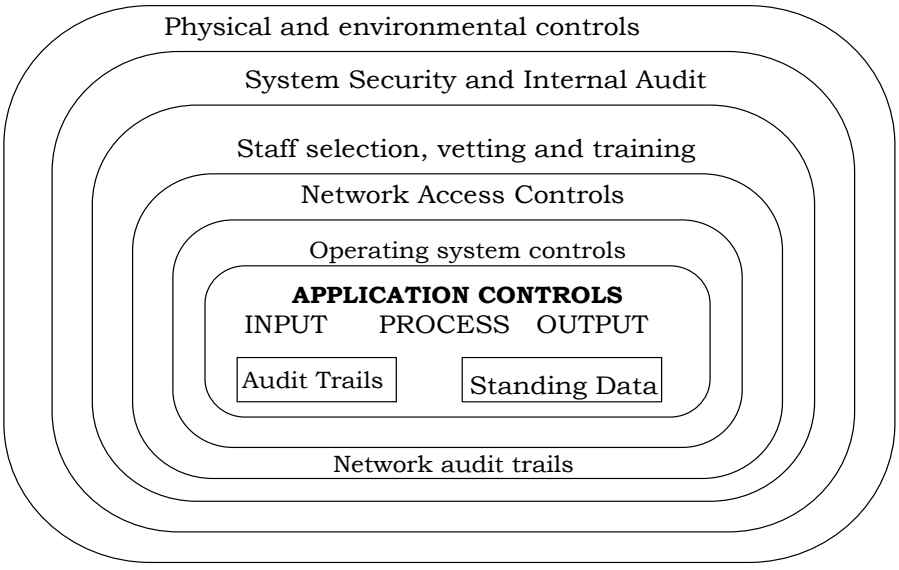
  All theses controls so far have been connected to the application. We have assumed that the person inputting the transaction is a competent, diligent and honest employee. This may not be the case. As we progress to the outer layer of the onion we find the more general IT controls which are aimed at:

  - preventing an unauthorised person gaining access to the system. This is becoming increasingly important with the growth in wide area networks and connection to the Internet;

- ensuring that the correct programs are being run on the computer systems. The auditor should gain assurance that the client has used the correct version of the accounting package, and not the untested version that may contain programming errors.

- Operating system controls: these can control which members of staff can access which application. For example, financial applications are usually run on a client's central computer system along with many other programs, e.g. personnel, word processing, manufacturing control systems etc. The operating system should have controls to ensure that only those with legitimate access to the finance systems should be able to use those applications. This is done with logical access security.
- Network Access controls : the vast majority of financial systems are connected to either a LAN or a WAN. These network connections need to be controlled to ensure that unauthorised users cannot gain access to the systems.
- System Security and Internal audit : These controls normally appear in the form of a systems security officer and an internal audit department. Their actions should assist in the identification of risks and the adoption of measures to reduce the risks to an acceptable level.
- Staff selection, vetting and training : Staff selection procedures and other personnel procedures should reduce the risks of errors etc by ensuring that staff are honest, reliable and that they know what they are doing.
- Physical and environmental controls : computers are both sensitive to their environments and attractive to criminals (in terms of their inherent value of the various components and the financial resources they control). The computers need to be physically protected from these risks.
- Sitting on top of all these controls is management's policies and standards. These should be policies and standards on all the inner rings of the control onion.

The IT controls framework



4 Planning an IT controls review

4.1 Knowledge of the entity

In addition to the knowledge of the auditee IT systems gathered at the planning stage (this has been covered in the "Introduction to IT audit" module), the auditor should obtain a detailed knowledge of the client being audited and the environment in which it operates, in order to perform a controls review. An integral part of gaining this knowledge is the gathering of information on the client's computer systems, since without such information the auditor would be unable to say that a full understanding of the client has been achieved.

Typically, gaining a knowledge of the client's computer systems will include gathering information on several aspects of the client's systems. This knowledge will allow the auditor to make an assessment of the complexity of the systems to be reviewed. This will in turn have an impact on the skills and resources required to carry out the review. For example, if the auditor finds out that the client has a large IT department with IBM mainframes running MVS, RACF and Oracle Financials, then the auditor may need to consider calling in additional resources such as an MVS specialist or at the very least start reading up on the MVS operating system.

The expression forewarned is forearmed is applicable when reviewing computer systems. Knowing what the client uses prior to a detailed IT controls review will allow the IT auditor to gather useful background and technical information.

The information gathered by the auditor should include:

- type of hardware used by the client to run its financial systems. For financial audit purposes the auditor will only be concerned with gathering data on those systems which are involved in the financial accounting processes. For example, if the client uses computers for market research which are separate from the accounting systems; the financial auditor would not need to look at these computers;
- system software (operating system , utilities, security software and networking software);
- financial and other applications : the auditor should determine which applications need to be reviewed as part of the audit process. For example the audit of a full set of commercial style accounts (income and expenditure account plus balance sheet) may require the auditor to look at an income an expenditure application, a payroll system and a fixed assets application;
- key client staff in both the finance and IT departments. The IT auditor will probably need to contact and interview these staff when carrying out a detailed controls review.

The IT auditor will also need to know:

- whether there have been any problems with the client's IT systems. For example, in previous years the client's system may have been unable to produce a complete trial balance;

- what changes, if any, are planned for the IT system. The auditor should avoid the situation where s(he) turns up at the client's premises and discovers that a new financial system has only just been installed.

The sources of information (this has also been mentioned in the "Introduction to IT Audit" module) should include:

- last year's working papers : the auditor should confirm that the information remains up to date and accurate;
- observation: touring the client's computer facilities;
- interviewing IT personnel;
- reviewing internal audit reports; and
- key client documents (the IT strategy, the business plan, expenditure profiles).

During the planning phase the IT auditor will only be aiming to get a high level overview of the client's systems.

4.2 Nature, extent and timing of audit procedures

When planning an IT review, the IT auditor will need to consider the audit approach. This will include an assessment of which systems need to be reviewed and when.

When determining which systems need to be reviewed the IT auditor should bear in mind:

- the contribution made by each system to the figures in the financial statements, or the importance of the non-financial IT system (systems can be classified as core systems/ mission-critical systems e.g. airline reservation systems, online trading systems, bank account management systems and support systems e.g. payroll, inventory, HR etc.)
- the size and complexity of the computer systems;
- the audit objectives;
- critical or important areas (identified by both the IT auditor and the financial auditor); and
- known weaknesses in internal control.

The timing of the IT review audit will dependent upon the auditor's requirements. For example, the financial auditor is most likely to ask the IT auditor to carry out a review as an input to the financial audit plan. The IT auditor will then have to prepare an IT audit plan, carry out the IT review and feed his/her findings into the financial auditor's overall risk assessment.

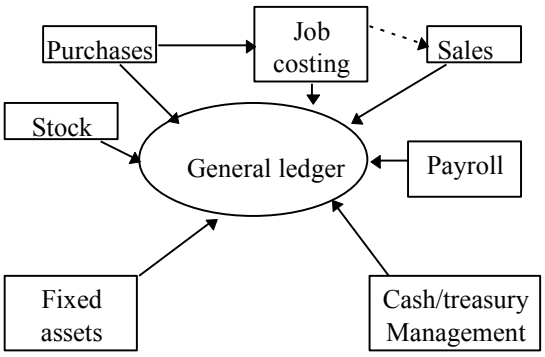
5 Documenting IT systems

5.1 Introduction

The auditor needs to document his/ her understanding of the IT system (and the associated control environment) in considerable detail.

For example, a financial accounting system could possibly have the following sub-systems/ modules:

- sales ledger;
- purchase ledger;
- stock management;
- cash management (receipts and payments);
- asset management systems (automated fixed assets registers);
- treasury management systems;
- payroll systems;
- grant management systems; and
- job costing systems.



Once an understanding of the transaction flows has been determined the auditor should review the systems of internal control.

Auditors should provide evidence of their understanding of the system by documenting both the transaction flow and the internal controls which operate on the transactions as they move through the accounting system.

Cross referencing to supporting documentation should be used where necessary.

The level of detail required when carrying out a review of a system will be dependant upon the scope and purpose of the audit.

If the auditor believes that a controls reliant audit approach is feasible, i.e. reliance will be placed on the client's systems of internal control, a more detailed controls review would be carried out. The level of detail is a matter of a professional judgement and the operating practices within each SAI. The review should be detailed enough to show how transactions are initiated, processed and recorded in the accounting records, together with the identification of internal controls at each stage.

However, if the auditor believes that a substantive audit approach is most likely, (from past experience, prior knowledge of the systems operated by the client), then the auditor still needs to gain a basic understanding of how the system processes and records transactions. This basic understanding can be documented using high level narratives or simple flowcharts.

The auditor can gain an initial understanding of how the system operates by performing certain tasks. For example:

- discussion with:
  - the client how the financial systems contribute to the business and the production of the financial statements;
  - previous auditors, e.g. last year's financial audit team.
- obtaining copies of:
  - organisation charts, showing lines of authority and separation of duties among IT and finance personnel;
  - charts of accounts, showing the major classes of transactions;
  - procedure manuals and desk instructions which describe approved working practices;
  - job descriptions.
- internal audit reports and working papers; and
- obtain copies of accounting records, input documents, standard proformas, documents, system reports etc.

The auditor should prepare an overview of the system which depicts the main elements and transaction flows. The accuracy of the overview should be confirmed with the client.

After documenting the system, the auditor should verify that that the system operates as described by carrying out walk-through tests. Walk-through tests are done by selecting a few transactions and tracing them through the system. Each documented step in the processing cycle is compared to the auditor's documented understanding of the system. Where differences are found the auditor's documentation should be updated.

5.2 Methods of documentation

There are several documentation techniques the auditor can use to prepare a description of the client's financial systems. These include:

- flowcharting;
- narratives; and
- questionnaires.

The choice of one or other particular technique will vary according to local auditing practices, the auditor's personal preferences and the complexity of the client's systems.

5.3 Flowcharting

Flowcharting is a means of graphically (diagrammatically) recording and describing the accounting systems. A flowchart can be used to show where internal controls operate within a transaction processing cycle.

Flowcharts are often most effective when they are produced in a top down perspective, i.e. they start at a high level by summarising the transaction flows and are followed by lower level flowcharts which expand upon the stages/procedures in the summarised flowchart.

Flowcharting is often preferred because:

- brevity : the auditor can use a flowchart on one sheet of paper to describe a system which if described in narrative would take many pages. Information is presented in a concise visual form rather than in longhand text;
- in more complex systems the use of flowcharts is preferable since they tend to be easier to understand and review. People tend to prefer a diagrammatic description;
- the use of flowcharts makes it easier to understand the flow of transactions through the processing and recording cycle from start to finish;
- inconsistencies and omissions are more apparent;
- it is often easier to analyse relationships between different procedures and transactions and therefore identify controls and deficiencies. Flowcharting is better at showing the span of each control; and
- updating of flowcharting is usually simpler than updating narrative.

As well as there being advantages to using flowcharting techniques, there are also disadvantages, for example:

- staff training may be required to avoid confusing or poorly prepared flowcharts;
- the auditor may be tempted to include too much detail into the flowcharts, wasting time making them perfect or, making them difficult to understand. A flowchart of a complex system can confuse more that it explains;
- they can be limited in scope and may not identify managerial or organisational controls;
- flowcharting conventions and symbols are not uniform and may vary from organisation to organisation; and
- they can be time consuming to prepare.

There are several flowcharting techniques available to the auditor. There are even standard off -the-shelf software packages which can be used to record and print a flowchart of the client's systems using standard symbols and stencils.

Whatever flowcharting method is used the auditor should bear in mind the following principles:

- standardised charting techniques and symbols should be used to make understanding review and update of the flowcharts easier;
- the flowchart should be relatively simple, concise and easy to understand;
- flowlines should, as far as possible, run from left to right and from top to bottom;
- diagonal lines should be avoided;
- try to avoid intersecting line (use a bridge symbol where this is not possible);



- significant copies of documents should be explained and accounted for, e.g. multiple copies of invoices;
- departments, sections or operating units should be represented by vertical bands across the flowchart, and operations should be depicted within the department to which they relate. Each columns should be headed up with an appropriate description , e.g. finance department; and
- narrative should be included, but kept to a minimum. Where detailed explanations are required, they should be attached as appendices.

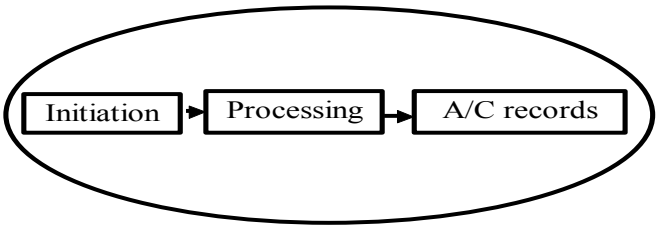
Since flowcharts should record the whole transaction lifecycle from transaction initiation to posting to the ledgers, they should include both manual and computerised procedures and controls. The IT auditor should ensure that his/her work on the computerised elements of the system can be linked in the work carried out by the financial auditor on the manual system procedures.

5.3.1 Common flowcharting techniques

This chapter includes coverage of a common flowcharting technique. Before moving on to what each of the symbols mean there are a few stages related to transaction processing which need to be explained in any systems description.

1. Initiation : when the transaction actually occurs and therefore needs to be recorded.
2. Data capture: where information is captured by the accounting system.
3. Data entry : when and how the transaction information is input into the transaction recording system.
4. Processing : how the financial system gather all the transaction information together and records details in the accounting records.

5. Accounting : the summarised transaction information produced by the system. Used as a basis for preparing the financial statements.



The auditor should bear in mind "when does the transaction legally occur?" and "when should it be recorded in the accounts?"

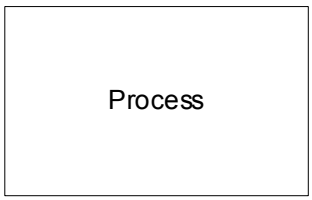
For example, when ordering goods in a purchasing system, what should be recorded when:

- the purchase order is completed;
- the purchase order is sent to the supplier;
- the goods are received; and
- the payment is made.

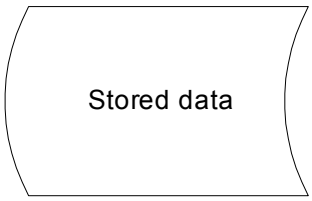
Exactly what information is recorded is dependant upon the client's accounting convention, e.g. commitment accounting, cash accounting or accruals accounting.

SYMBOLS

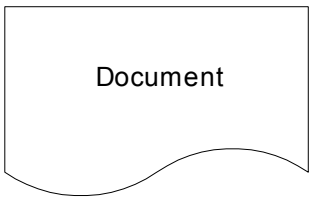
The large box represents a processing task. The task an be performed by either a person or a computer. For example a process could be "bank the cash" (manual) or "update the masterfile records" (automated).



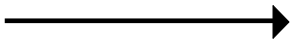
This symbol is a computer file e.g. a vendor details file which contains the vendors name, address and bank account details.



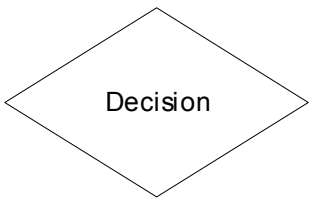
This symbol represents a document or a report. The report could be either computer or manually produced.



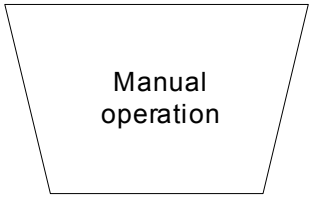
The arrow symbol is used to show the direction of flow of data. For example, if a process results in a report being produced, the line would be from the process symbol to the report symbol. If the data flows both ways, then the arrow would be at both ends, e.g. if a process reads a masterfile and then updates it.



The diamond shaped symbol can be used to represent a decision being taken.



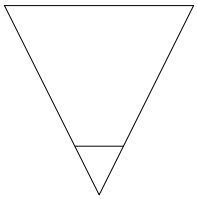
The trapezium shape is used to represent a manual process carried out without mechanical aid.



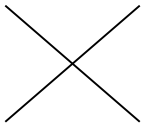
A parallelogram is used to represent data input and or data output.



A triangle is used to represent a document or paper file, with a letter in the middle indicating which order the papers are filed, e.g. N=numerical order, D=date order, A= alphabetical order.



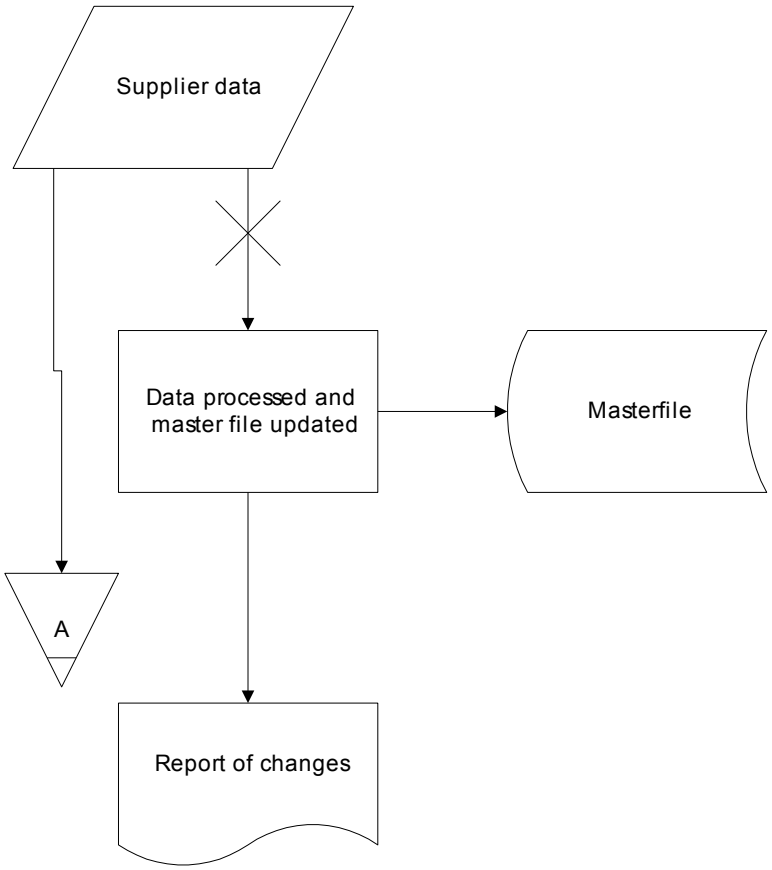
A cross is used to represent an operation performed by client staff, e.g. clerical activities.



Preparing a flowcharts normally starts with the initiation of a transaction., i.e. at the very start of the transactions cycle.

The following provides a simple illustration of a simple flowchart.

A computer user receives a form containing data on suppliers, checks that the data is complete, and enters it into the financial system. The data form is filed alphabetically. The computer processes the input data and accesses the supplier masterfile. The masterfile is then updated and a report is produced.



5.3.2 Flowcharting case study

The following describes a transaction processing system. Draw a flowchart to illustrate the stages in transaction processing.

1. Requisition order is raised by the stores department when the level of stores drops below a predefined level.

2. Requisition order is signed by the stores manager. The order is sent to the buyer section of the finance department.

3. The buyer checks the signature on the requisition order .

4. The buyer fills in a purchase order, using a supplier from the approved list. Part 1 is sent to the supplier, part 2 is filed numerically, part 3 goes to the goods inwards section.

5. The buyer files the requisitions in date order.

6. When goods are received they are checked to the purchase order. If not the same the foods are rejected. If delivery is correct a goods received note is raised. Copy 1 is filed in numerical order. Copy 2 is sent to the buyer.

7. The buyer checks the signature on the goods received note and checks the details to the filed purchase order. The GRN is placed in a temporary file.

8. The supplier sends an invoice to the accounts department. The invoice is stamped and numbered sequentially. The invoice is sent to the buyer.

9. The buyer files the invoice until the GRN arrives. Once received the invoice is matched with the goods received note.

10. Buyer enters account code and signs for approval.

11. Finance review the invoice to ensure approved and account number added.

12. Payment added to payments list for subsequent payment.

5.4 Narrative descriptions

Written descriptions of the transaction processing cycle are also used to document systems. Narrative descriptions are often used in conjunction with the other methods of system documentation.

Narrative descriptions should include:

- system objectives and targets;
- processes and procedures;
- links and interfaces with other systems;
- controls : what they are, spans of control;
- what happens when exceptional conditions occur; and
- ad hoc controls, e.g. management review and supervision.

As with flowcharting, there are both advantages and disadvantages associated with this method of documentation.

Advantages include:

- they provide details of the procedures and controls in operation;
- they can, for smaller systems, provide a precise, coherent description of the system, including strengths and deficiencies;
- they can be prepared in a short time;
- auditors don't require extensive training to be able to prepare a narrative description of a client's system; and
- they are useful when describing transactions that are treated in a unique or special manner (i.e. describing the unusual transactions).

The disadvantages of this method include:

- narrative descriptions can be cumbersome, especially when attempting to describe a large system;
- they can be difficult to interpret;
- interrelationships may not be clearly shown. It is more difficult to show control interactions or the spans of controls, for example, if a control on one page of the narrative description mitigates a control weakness on another page.

5.4.1 Example of a System Description:

Inventory Cycle

Upon receipt of the inventory from the receiving department, the stores clerk enters the information into the inventory receipts subsystem. Once the receipt is complete, the subsystem verifies the item's part number to the inventory master file. If the part number doesn't exist, the stores clerk either enters in the new number or corrects the entry. For new entries, the inventory master file is updated and a new updated report printed.

The inventory receipt subsystem then updates the inventory quantity file and prints the report for that part number. The report is then agreed to the input information, (a signature provides the evidence of performance of the procedure) and filed.

The stores clerk receives the day's issues from the sales department through the inventory requisition subsystem. The quantity is verified and removed from inventory. The module updates the inventory quantity file and prints a report for the particular part number. The report is then agreed back to input information, signed evidencing performance of the step and filed.

A store issue chit is also printed. The receiver of the inventory signs the chit evidencing acceptance of the items. The chit is then filed.

Access to the inventory application subsystems is restricted to the stores clerk. Also, the stores terminal is the only terminal that can access the application program.

All documents are numerically sequenced. Computer edit routines verify document sequencing and also perform key field checking.

5.5 Questionnaires

Questionnaires consist of a series of questions about the client's accounting systems. Whilst they do not document transaction flows, they can assist the auditor in gathering information on the client's systems, and in particular the control procedures. Questionnaires can assist the auditor in making enquiries, and can provide assurance that all the significant issues have been covered.

A common type of questionnaire is the internal control questionnaire (ICQ). These are used to evaluate internal controls and the strengths and weaknesses within a client's systems.

ICQs normally list questions related to specific control objectives that might be expected to be present in a system. The questions should be grouped together under related control objectives. For example there may be a group of questions which are aimed at determining if there are adequate controls to reduce the risk of transactions being lost (i.e. the risk to the completeness objective). If there are controls in place the auditor may be able to rely on them (after testing them), and hence reduce the amount of substantive testing required to satisfy the auditor's completeness objective.

ICQs normally require the auditor to enter a yes/no answer in response to a question, e.g. are computer input documents required to be authorised.? A space is left for any comments the auditor may have.

When using an ICQ the auditor should bear in mind that the questions are aimed at the auditor, NOT the client. If the ICQ asks a question about authorisation of input documents, the auditor should ask the client an open question such as " what procedures are there to authorise input documents?" The auditor should assess the client's reply and then decide if the control objective is satisfied.

Questionnaires can be pre-printed to serve as an audit guide. They ensure a consistent approach when collecting information on the client's computer systems and computer controls. Where pre-prepared ICQs are used, the IT auditor should be aware that the questions may need to be adapt as the review progresses. The auditor should also ensure that the questions are relevant to the client.

Points to consider when using ICQs:

- the questionnaires prompt for yes no responses which may not reflect the complexity of a client's system;
- ICQs can become very large and cumbersome, requiring considerable time to complete;
- they can encourage a mechanistic unimaginative style of audit which ignores the auditor's instincts; and
- factors particular to a client may not be reflected in the ICQ.

Within the scope of the IT auditor's work, questionnaires or proformas can also be used to document background and other client related information, e.g. on the hardware and software used by the client.

6 Organisation and management controls

6.1 Introduction

This chapter covers the high level controls adopted by management to ensure that the computer systems function correctly and that they satisfy business objectives. Our aim, as external auditors, is to determine whether the controls that the client has put in place are sufficient to ensure that the IT activities are adequately controlled. In carrying out our assessment we cover the following areas:

- risks associated with inadequate management controls;
- IT organisational structures;
- IT strategy and senior management involvement;
- personnel and training policies;
- documentation and document retention policies;
- outsourcing policies;
- internal audit involvement;
- IT security policies;
- legal and regulatory compliance; and
- segregation of duties.

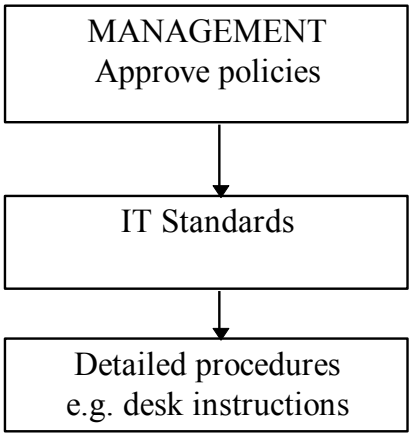
In principle, the organisation and management issues which are relevant to an IT function are no different from those within a client's finance function. The underlying principles are the same.

Experience has shown that high level IT policies, procedures and standards are very important in establishing a sound internal controls framework. Clients which do not have robust high level IT organisation and management controls are unlikely to have adequate lower level, detailed controls.

The high level policies are important as they establish a framework on which the client can develop lower detailed controls.

It is a general rule that controls flow from the top of an organisation down (after all controls are ultimately senior management's responsibility).

The flow of controls can be illustrated in a diagrammatic form.



Management establishes and approves the policies. The policies are usually high level statements of intent.

The policies then feed down into standards.

Detailed procedures (and controls) flow from the standards.

Note : when reviewing a client's IT policies and standards, the auditor should bear in mind that each client is likely to be different and have different organisational and management requirements. The auditor may assess whether the client's organisational structure and the place of IT within the structure is appropriate.

The auditor would loose credibility if s(he) made purely theoretical criticisms without paying any regard to the client's circumstances. For example, recommending that the client employs more staff to increase segregation of duties within the IT department.

6.2 Risks associated with inadequate controls

6.2.1 Risks

- management has ultimate responsibility for the safeguarding of the organisations assets. They are responsible to stakeholders; taxpayers and every citizen in the public sector, and shareholders in the private sector. Management sets policies to ensure that the risks to the assets are adequately managed;
- inadequate management involvement may lead to a direction-less IT function which, in turn does not serve the business needs. This may give rise to problems with the financial systems being unable to meet new reporting requirements (which may occur due a change in national accounting standards, or a change in Government requirements);
- poor reporting structures leading to inadequate decision making. This may affect the client's ability to deliver its services and may affect its future as a going concern (one of the fundamental accounting principals);

- inappropriate or no IT planning leading to business growth being constrained by a lack of IT resources; e.g. the IT manager reports to the chief executive that the system is unable to cope with an increase in sales. Overloading a computer system may lead to degradation or unavailability through communication bottle-necks or system crashes;
- ineffective staff who do not understand their jobs (either through inadequate recruitment policies or a lack of staff training or supervision). This increases the risk of staff making mistakes and errors;
- disgruntled staff being able to sabotage the system, for example when staff find out they are going to be disciplined or made redundant; and
- ineffective internal audit function which cannot satisfactorily review the computer systems and associated controls;
- loss of the audit trail due to inadequate document retention policies (includes both paper and magnetic, optical media); and
- security breaches leading to data loss, fraud, and errors.

6.3 IT organisation and structure

This chapter continues with a look at how IT fits into the client's management structure.

Within a typical IT department the chief executive, (or board of directors, management executive, senior management board) should occupy the top of the chart, emphasising the importance of IT to the organisation.

Error! No topic specified.

Next we move on to see how a client's IT department fits into the overall organisational structure, including the links with other parts of the business.

Error! No topic specified.

The IT director should be a member of the IT steering committee. Membership will allow him/her to discuss the IT strategy and any IT related problems with the system users. Feeding into the IT steering group will be various project teams and representatives of user departments.

A large client may have a security committee which reports to the chief executive. The IT security officer would report to the security committee.

6.3.1 Senior management control and involvement

Issues to consider when reviewing the organisation and management controls within a client's IT department.

Overall responsibility : This includes a review of how IT fits into the overall organisational structure. The auditor should determine if there is a board member or senior manager (someone with senior management influence) with responsibility for IT. If such a person does not exist there is an increased risk that IT will not be given the recognition, attention or

resources it requires to meet the business objectives. The external auditor will be concerned if the financial systems are not given the resources required to produce complete and accurate accounts.

Formal IT structure: There should be a formal organisation structure with all staff knowing their roles and responsibilities, preferably by staff having written down and agreed job descriptions.

IT steering committee : ideally there should be a steering committee which comprising of user representatives from all areas of the business, and IT personnel. The steering committee would be responsible for the overall direction of IT. The nature of the IT steering committee will vary according to the client's circumstances. For example, a large Government department would be expected to have a formal IT steering committee, whilst in a small client, the IT steering committee may be small and informal. The IT steering committee would be responsible for issues beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

To be effective, the IT steering committee should draw its members from senior and middle management. Membership should be drawn from all user departments within an organisation. Senior management's place is especially important since their presence gives the decisions made by the committee greater weight.

The role and functions of steering committees, are covered in greater depth in the INTOSAI developing systems module.

6.4 IT Strategy

Once the steering committee agrees on a future direction for IT, the decisions should be formalised and documented in a plan. The future direction agreed by the IT steering committee is normally set out in a document known as the IT strategy.

The IT strategy is in effect the starting point for any investment in IT as it identifies future changes which have to be budgeted for.

The decisions and planned changes specified within the IT strategy would then feed into the IT department's annual plans.

Although the IT strategy is likely to have a minimal effect on the current year's audit it may have a significant effect on future years' audits. A review of a client's IT strategy could forewarn the IT auditor of problems which may arise in later years. For example, the IT strategy may state that the organisation will replace its financial system in two years time. This may have an impact on the work of the auditor.

From the client's point of view, the main risk associated with a poor or absent IT strategy is the development of systems which do not meet business needs.

When reviewing the IT strategy we should look for the following:

- the IT strategy should follow the business strategy: In the past IT departments were in control of IT spending decisions. This resulted in IT systems being installed because the technical staff wanted new systems, instead of because the business required new systems;
- it is becoming increasingly common for IT to be seen as a business expense which must justify itself. Consequently all major IT expenditure is scrutinised and investments are only made where there is a strong business case;
- the IT strategy should be forward looking. They typically look 3 years into the future. It is difficult to accurately predict any further because of the pace of technological change;
- the pace of change also means that the IT strategy should be reviewed annually to check that its assumptions and decisions remain valid;
- awareness: staff should be kept informed of the main issues in the IT strategy;
- the strategy should include consideration of the finance systems; and
- the strategy should be approved by senior management.

The size, detail and content of a client's IT strategy will vary according to various factors including : the size of the client and its IT department; and the importance or criticality of the IT systems.

For example, a large government departments or ministries are likely to have detailed IT strategies which span several hundred pages within many volumes. At the other end of the scale, a small client's IT strategy might comprise of a one or two page document.

When reviewing the client's IT strategy the auditor should consider what is appropriate for the organisation.

IT strategies are covered in more depth in the developing systems module of the INTOSAI IT audit course.

6.5 Personnel and training

In terms of frequency of occurrence, the most common causes of data loss, unauthorised data and program amendment, and system crashes are:

- errors and omissions caused by people;
- natural disasters (flood, fire, storm, earthquake, lightning strike, or just a simple powercut);
- fraud; and
- hardware/software failure.

Errors and omissions are the biggest source of problems. It is therefore important that the client has controls and procedures in place to reduce the risk of mistakes being made. This may be achieved through the adoption of appropriate personnel policies and procedures, for example:

- a clear organisational structure supported by reporting lines/ charts;
- job descriptions;
- staff planning;
- training and staff development;
- hiring/firing policies (including codes of conduct);
- staff assessments (promotion/demotion);
- special contracts;
- job rotation; and
- staff vacations.

6.5.1 Organisational charts

There should be organisational charts which show lines of reporting and management. This should ensure that all staff know how they fit in to the organisational structure of the business and the IT department. The charts also provide an indication of who staff should inform when they encounter problems.

6.5.2 Job descriptions

All IT staff should be given job descriptions. These should describe what tasks the IT staff should perform as part of their jobs. They can be used for staff evaluation and assist the auditor in determining whether there is adequate segregation of duties.

6.5.3 Staff planning

Staff planning is important to ensure that there are enough appropriately skilled IT personnel to run the current systems as well as meet future staffing requirements. Examples of the need for staff resource planning include:

- where a client has decided to upgrade their computer systems, staff who are considered to be experts in the old system may feel that their value to the organisation has diminished or even that their days of employment are numbered. Consequently they may feel demoralised and may not support the old systems adequately;

- when installing new systems the technical skill necessary to run the new system may not be available. Management may need to identify skills requirements up front and send staff on training courses, recruit new staff or hire consultants for a period.

6.5.4 Training and staff development

Staff training and development are closely linked to staff resource planning. IT management should know what staff skills are required in both the present and the foreseeable future. Staff should be given the training to meet those requirements. The need for training is ongoing as

both hardware and software continually develops. IT training is often costly and should be controlled by training plans and budgets.

To reduce the dependence on a few key employees the client may use a form of cross training, i.e. training members of staff to carry out the jobs of their colleagues in the event of absence. It also provides for a form of succession planning. The client should be aware that training staff to fill in for another staff member increases the risk that those staff will have a more detailed knowledge of the whole system, including the existence of any compensating controls.

6.5.5 Staff recruitment/termination policies and codes of conduct

The policies should apply to the employment of permanent staff, temporary staff, contractors and consultants. Staff hiring policies should be adopted to ensure that appropriate staff are chosen. There should also be policies and procedures to deal with the other end of the employment cycle, i.e. termination (whether voluntary or compulsory). The policies are likely to be heavily influenced by legal requirements, i.e. the employment legislation within each country.

When hiring new members of IT staff, the client would be expected to take account of:

- background checks : including taking up references (in some countries it may be possible to check for criminal convictions);
- confidentiality agreements : these state that the employee will not reveal confidential information to unauthorised third parties; and
- codes of conduct, including contractual relationships with relatives, the acceptance of gifts, conflicts of interest etc.

New employees should be made aware of their roles and responsibilities in respect of security matters.

Termination policies should define the steps to be taken when an employee's services are no longer required. It is important that these policies and procedures are in place because of the considerable damage a disgruntled employee can cause to a computer system. Termination policies should address:

- voluntary termination (resignation, retirement);
- involuntary termination : i.e. being sacked;
- immediate termination, e.g. due to gross misconduct;
- security measures: which may include:
  - the return of access keys, id cards and badges;
  - deletion or deactivation of logical access privileges, e.g. their password.
- other procedures:

- notification of other employees. Other employees should be aware staff termination's and they will be more aware of any unauthorised activities that those employees may try to carry out;
- arrange final pay routines to ensure that that person is removed from the payroll;
- leaving interviews may be useful in determining the terminating employees feeling toward the organisation;
- return of company property, including personal laptop computers, pagers, smartcards etc; and
- escort off premises (if required).

6.5.6 Staff assessment, including promotion and demotion

Staff assessment policies and procedures should be seen to be fair and equitable. and understood by all employees. The policies should be based on objective criteria and consideration should be given to all relevant factors, which may include: the staff member's education, training, experience, level of responsibility, achievement, and conduct.

6.5.7 Special contracts

It is increasingly common for IT departments to call in specialists, contractors and consultants for one off jobs. There should be policies which require those on special contracts to adhere to established policies and procedures.

6.5.8 Job rotation

Job rotation can provide a degree of control because the same person does not carry out the same duties all the time. Job rotation allows other staff to perform a job normally carried out by another person and can lead to the detection and identification of possible irregularities. Job rotation also acts as a preventive control. Staff are less inclined to adopt unapproved working practices or commit frauds if they know someone else is taking over the job.

6.5.9 Required vacations

Staff should be required to take regular vacations, at least once a year. This should reduce the risk of unauthorised or illegal acts remaining undetected. Required vacations may be a condition of insurance in some businesses, e.g. the banking industry. There have been cases where staff have not taken leave for several years and carried out frauds involving teeming and lading. Their frauds have only been discovered when they have fallen ill and their work undertaken by another employee.

6.6 Documentation and document retention policies

When reviewing a client's systems of internal control, the IT auditor can gain much of the information s(he) requires from client documentation. The auditor may also need to examine client documentation to test individual transactions and account balances.

6.6.1 Systems documentation policy

The risks associated with inadequate documentation policies include:

- unauthorised working practices being adopted by IT staff;
- increase in the number of errors being made by IT staff;
- systems which are difficult to maintain, thereby increasing the risk of system unavailability. For example if a client's network is not adequately documented and a problem occurs with the wiring, those tasked with carrying out repairs would have difficulty in locating where the failure had occurred. They would not be able to determine which floorboard the cabling was under.

The policy on documentation should state that all system documentation should be kept up to date and that only the latest versions should be used. The policy may also state that backup copies of documentation should be stored in a secure off-site location.

Some clients may have decided to adopt the international quality standard ISO 9001, "Quality systems : Model for quality assurance in design, development , productions, installation and servicing". Other clients may have achieved certification under the other ISO 9000 quality standards.

Where a client complies with this international standard, there should be policies on document production, approval and issue, as well as on policies on controlling changes to existing documents.

6.6.2 Document retention policies

The auditor may need to examine evidence in order to reach an opinion on the financial statements. Historically, this evidence has been obtained from paper documents (invoices, purchase orders, goods received notes etc). As more clients install computer systems, the auditor will find more evidence in the form of electronic records.

Ultimately, if the client does not retain sufficient, appropriate evidence the auditor would have difficulty in being able to provide an unqualified audit opinion.

The auditor should consider two types of documentation according to the audit approach:

Controls reliant audit approach : the auditor would require evidence of controls in operation during the accounting period. This evidence may consist of reconciliations, signatures, reviewed audit logs etc.

Substantive testing : assurance may require the auditor to examine evidence relating to individual transactions. The auditor may need to be able to trace transactions from initiation through to their summarisation in the accounts. Where transaction details are recorded in computer systems they should be retained for audit inspection. Where storage space is scarce e.g. limited capacity on hard disks, the client may archive data or summarise transaction data into balances. If the client archives data, the auditor may need to ask for it to be retrieved before s(he) makes a visit. If the client summarises transactions into balances the auditor will

need to find or request an alternative audit trail, e.g. asking the client to produce a hard copy of the transactions which make up the summarised balances.

There may be other, non audit, requirements which require the client to retain transaction documentation, e.g:

- import regulations;
- taxation regulations; and
- company legislation requirements.

The client's documentation retention policies should take account of all these requirements.

6.7 Outsourcing policy

There is an increasing trend for IT services to be delivered by third party service providers. This has arisen because IT is not seen as being a core business activity. Management may take the attitude that their business involves the delivery of products and services, and not the provision of IT services. Outsourcing allows management to concentrate their efforts on the main business activities.

The need for outsourcing may also be driven by the need to reduce running costs.

Where a client outsources or intends to outsource its IT activities the auditor should be concerned with reviewing the policies and procedures which ensure the security of the client's financial data.

The auditor may need to obtain a copy of the contract to determine if adequate controls have been specified.

Where the client intends to outsource its IT function the auditor should ensure that audit needs are taken into account and included in contracts. Contract terms are frequently difficult to change once they have been signed. Even if the third party is willing to amend the contract it is likely to charge a large fee for doing so. The fee may be passed on by the client to the auditor.

Detailed controls associated with third party service providers are considered later in this module (chapter 13).

6.8 Internal audit involvement

As mentioned previously in this module, management has ultimate responsibility for ensuring that an adequate system of internal controls is in place. Management puts policies and procedures in place and gets assurance that the controls are in place and adequately reduce identified risks by relying on the review work carried out by internal auditors.

The external auditor can view the client's internal audit function as part of the overall control structure (since they prevent, detect and correct control weaknesses and errors).

The external IT auditor should carry out a general assessment of the client's internal audit function. This assessment will enable the auditor to decide if we can use or place reliance on internal audit's work. The external IT auditor should determine if:

- assurance can be taken from the internal audit activities;
- internal audit staff can be used to provide direct audit assistance, if necessary under the supervision of the external auditor. For example the external auditor may ask the internal auditors to assist with checking the existence of fixed assets.

Before placing reliance on the IT controls review work carried out by the client's internal audit, we should carry out our own assessment of their work. This assessment may be largely informed by past experience and direct examination of internal audit's work. Basic questions the external auditor may ask when reviewing internal audit's work include:

- does internal audit report to senior management?
- can internal audit report to the board and, or audit committee?
- are management required to act on internal audit's recommendations?
- is it empowered to carry out a full range of assessments or are there significant restrictions on the scope of its work?
- are there sufficient resources available, in terms of finances and staff? and
- is the quality of internal audit's work acceptable, in terms of planning, supervision, review and documentation?

Staff with IT audit skills and experience will not always be employed by internal audit departments. Some internal audit departments may have in-house IT audit staff, others may contract in IT auditors for specific reviews. Some internal audit departments may not carry out any IT controls reviews.

The external auditor should consider whether the IT audit department has the staff necessary to carry out competent reviews on the client's computer systems.

Should the external auditor intend to place reliance on the work of internal audit s(he) should review the work to the SAI's own auditing standards.

6.9 IT security policy

It is important that the client establishes an IT security policy which clearly states the organisation's position. The lower level, detailed controls should be based on the IT security policy. For example, detailed password controls would be based on the logical access section of the IT security policy.

IT security policies are normally expressed in the form of a concise narrative, i.e. a few pages of text.

The policy requires senior management approval if it is to have any weight, and consequently should be approved at board level or equivalent. The policy should be seen to be backed by senior management.

The policy should be available to all employees responsible for information security. Where the client has staff who have access to a computer system this will include all such staff.

The policy should contain the following:

- a definition of information security, its overall objectives and scope;
- a statement of management intention, supporting the goals and principles of information security;
- an expansion of specific security policies, principles, standards and compliance requirements including:
  - compliance with legal and contractual requirements;
  - security education and training;
  - virus prevention and detection policy;
  - business continuity planning policy.
- a definition of general and specific responsibilities for all aspects of information security; and
- an explanation of the process for reporting suspected security incidents.

The client should put in place methods for monitoring compliance with the policy and ensuring that the policy remains up to date.

The IT security policy should be supported by more detailed IT security standards and procedures. For example:

- the IT security policy would state that all computer systems should be protected by password controls;
- the IT security standards would say that the passwords should be 6 characters in length, be hard to guess and consist of a mixture of alpha and numeric characters; and
- the IT security procedures would provide users with guidance on how to change their passwords in the various systems they are authorised to use, e.g. the power-on password, the mainframe password etc.

Some clients set up information security forums to consider and co-ordinate IT security policies.

Responsibility for IT security is normally assigned to a security administration function. In smaller clients this function may be a part-time job carried out by a member of staff known as the IT security officer. Larger clients would be expected to have dedicated IT security personnel.

IT security is also covered in the INTOSAI IT security module.

6.10 Legal and regulatory compliance

The legal and regulatory requirements will vary from one country to another.

Legal and regulatory requirements may include:

- data protection and privacy legislation to protect personal data on individuals, e.g. their payroll information;
- computer misuse legislation to make attempted computer hacking and unauthorised computer access a criminal offence;
- banking and finance regulations, where banks may have to undergo regular reviews if they wish to continue operating; and
- copyright laws to prevent the theft of computer software.

The client should be aware of local requirements and have taken appropriate measures to ensure compliance.

Non-compliance could result in action varying from a warning letter to prosecution or even closure of the business. Where penalties are significant the client may make a breach of regulations or legislation an internal disciplinary offence.

6.11 Segregation of duties

Separation of duties is a proven way of ensuring that transactions are properly authorised, recorded, and that assets are safeguarded. Separation of duties occurs when one person provides a check on the activities of another. It is also used to prevent one person from carrying out an activity from start to finish without the involvement of another person. Segregation of duties reduces the risk of fraud since collusion would be required to bypass the control.

Segregated duties can also provide a form of error checking and quality control.

Separation of duties includes both:

- separating the responsibility for the controls of assets from the responsibility of maintaining the records which account for them; and
- separation of functions within the IT environment.

Separation of duties applies to both the general controls environment and to specific applications or programs.

Within the general IT controls environment, the various functions and roles within the IT department should be segregated.

For example, a software developer would not require access to the live computing environment to be able to carry out his or her job. Programming staff should not have the authority to transfer new software between the development, test and production environments. Segregation of duties between programmers an operations staff would reduce the risk of those with programming knowledge being able to make unauthorised amendments to programs.

In many cases the IT department will be divided into two broad types of activity:

- programming (systems and applications); and
- computer operations.

Staff should not have duties which fall into both types of activity. Programming staff should not be allowed access to live data files and programs.

In an ideal world most of the functions within the IT department would be carried out by different personnel. e.g:

- systems design and programming;
- systems support;
- routine IT operations;
- data input;
- system security;
- database administration; and
- change management.

With the pressure to reduce the cost of IT functions, staff numbers are often reduced. This limits the scope for segregated duties. If this is the case, then the auditor should adopt a pragmatic approach to identifying weaknesses and providing recommendations. Where the scope for segregated duties is limited the auditor should look for the existence of compensating controls such as strong computer security and end user reconciliations.

The auditor should determine if IT staff also have responsibilities in user departments. IT should be segregated from user functions such as finance, stock management, grant assessment etc. Staff with duties in both IT and a user area would have greater knowledge of the systems, including the existence of manual and compensating controls, and be able to make unauthorised changes which would be difficult to detect.

7 IT Operations

7.1 Roles and responsibilities of IT operations

The roles and duties of IT operations include the following:

1. capacity planning : i.e. ensuring that the computer systems will continue to provide a satisfactory level of performance in the longer term. This will involve IT operation staff having to make estimates of future CPU requirements, disk storage capacity and network loads capacity.

2. performance monitoring : monitoring the day to day performance of the system in terms of measures such as response time.

3. initial program loading : booting up the systems, or installing new software.

4. media management: includes the control of disks and tapes, CD ROMS (and punched cards if the client has a very old system).

5. job scheduling : a job is normally a process or sequence of batch processes which are run overnight or in background and which update files etc. Jobs are normally run periodically, either daily, weekly, monthly, quarterly or annually.

6. back-ups and disaster recovery : backups of data and software should be carried out by IT operations staff on a regular basis. Back-up and business continuity issues are covered in depth in a later chapter.

7. help desk and problem management : help desks are the day to link between users with IT problems and the IT department. They are the ones users call when they have a printer problem or they forget their password. Problems may be encountered with individual programs(applications and system), hardware, or telecommunications.

8. maintenance :of both hardware and software.

9. network monitoring and administration: the majority of computers used in business, including government, are networked. The IT operations function is given the responsibility for ensuring that communication links are maintained and provide users with the approval level of network access.

'Computer operations' refers to the logistic and infrastructure aspects of hardware and software. Appropriate computer operations shield users from the need to consider these matters by ensuring that the application systems are available at scheduled times, they operate as expected and the results of their processing, such as printouts, are produced on time. In a well run IT department, we expect to find computer operations that are transparent to users, fully supporting them in the performance of their roles.

7.2 Risks associated with poorly controlled computer operations

Risks include:

- applications not run correctly (wrong applications run, or incorrect versions or wrong configuration parameters entered by operations staff, e.g. the system clock and date being incorrect which could lead to erroneous interest charges, payroll calculations etc);
- loss or corruption of financial applications or the underlying data files : may result from improper or unauthorised use of system utilities. The IT operations staff may not know how to deal with processing problems or error reports. They may cause more damage then they fix;
- delays and disruptions in processing. Wrong priorities may be given to jobs;
- lack of backups and contingency planning increases the risk of being unable to continue processing following a disaster;
- lack of system capacity. The system may be unable to process transactions in a timely manner because of overload, or lack of storage space preventing the posting of any new transactions; and
- high amount of system downtime to fix faults : when the systems are unavailable a backlog of unposted transactions may build up;
- users' problems remaining unresolved due to a poor help-desk function. Users may attempt to fix their own problems.

7.3 Control of IT operations

7.3.1 Service level agreements

It is increasingly common for IT departments to draw up and agree service level agreements with the rest of the organisation, i.e. the user departments. This allows users to specify and agree, preferably in writing, what levels of service, in terms of quantity and quality, they should receive. SLAs are in effect internal service delivery contracts.

Without a service level agreement the following saying becomes relevant: "if you aim at nothing, that is usually what you hit."

The structure and level of service specified in a SLA will depend upon the working practices and requirements of each organisation. A typical SLA would contain the following :

- general provisions (including the scope of the agreement, its signatories, date of next review);
- brief description of services (functions applications and major transaction types);
- service hours (normal working hours and special occasions such as weekends and bank holidays);
- service availability (percentage availability, maximum number of service failures and the maximum downtime per failure);
- user support levels (help desk details);
- performance (response times, turnaround times);

- contingency (brief details of plans);
- security (including compliance with the organisation's IT security policy); and
- restrictions (maximum number of transactions, users);

The auditor should review any SLAs to determine that they support the accurate and consistent processing of financial data.

7.3.2 Management control, review and supervision

Operations staff should be supervised by management.

From the standpoint of separation of duties, operations staff should not be given the job of inputting transactions or any form of application programming.

The client's IT systems may have on them software utilities which could conceivably be used to make unauthorised amendments to data files. Operations staff with access to such software should be supervised to ensure that they only use the utilities for authorised purposes.

Management will be unable to provide continuous monitoring of operations staff and may place some reliance on the automatic logging and monitoring facilities built into the systems. The events which are recorded in the logs will depend on the parameters set when the systems were installed. As with most logging systems, a large quantity of data can be produced in a short period. Recommending that a client review the audit logs on a regular basis is unlikely to be carried out in practice. To assist management in their detection of unauthorised activity, the client should develop procedures (e.g. a program) to report exceptions or anomalies.

Effective supervision over IT operations staff is often difficult to achieve, due to their high level of technical knowledge. They could do things to the system which management would not detect , or even recognise the significance of, if they did detect a change. Therefore to a certain extent management must place a high degree of trust on IT operations staff, and that trust will be based on appropriate staff selection and vetting procedures (as per the organisational and management controls discussed in the previous chapter, {chapter 6}).

7.3.3 Training and experience

IT operations staff should have skills, experience and training necessary to carry out their jobs to a competent standard. The IT auditor should determine if the training needs of IT operations staff have been assessed. Training needs may include non-technical training, e.g. management training for IT operations supervisors.

As an aid to continuity of staffing, some organisations may teach staff more than one role or introduce a form of job rotation.

Closely connected to training is the career development of staff. If IT operations feel that they are in a dead end job with little scope for progression their morale may be low and they are less likely to carry out their work to a high standard (they may even be tempted to cut corners and carry out unauthorised activities).

7.3.4 Computer maintenance

As with most equipment, computers may require regular maintenance to reduce the risk of unexpected hardware failures. Although preventive maintenance is becoming less common, especially for mini and microcomputers, it may still be required for environmental equipment such as air conditioning units and fire extinguishing systems. The IT operations function should either have an internal maintenance capability, or contract out the maintenance to a third party supplier.

The IT auditor may wish to examine the maintenance contracts and schedules to determine if adequate maintenance is carried out. Ultimately the key test to the adequacy of the client's maintenance arrangements is the amount of system down-time or the number of Helpdesk incidents arising from equipment failures.

7.3.5 Operations documentation

The client should have clear, documented operating procedures for all computer systems to ensure their correct, secure operation. The documented procedures should be available for the detailed execution of each job, and should include the following items:

- the correct handling of data files;
- scheduling requirements (to ensure best use of IT resources);
- instructions for handling errors or other exceptional conditions which might arise when jobs are run;
- support contacts in the event of unexpected operational or technical difficulties;
- special output handling instructions; and
- system restart and recovery procedures.

The client should also have documented procedures for daily housekeeping and maintenance activities such as computer start-up procedures, daily data back-up procedures, computer room management and safety.

Documentation can be used by operations staff when they are unsure about how to carry out a procedure. They are also useful in training new staff.

The auditor should bear in mind the level and detail of documentation will vary from one client to another, and will depend on factors such as the size of the organisation, the type of hardware and software used and the nature of the applications. The auditor would expect to see large quantities of high quality documentation in a large, critical IT operation, whereas a small client running office automation software would probably have less detailed and extensive documentation.

7.3.6 Problem management

The IT operation section should have documented procedures for detecting and recording abnormal conditions. A manual or computerised log may be used to record these conditions.

Contents should include:

- error or fault detection date :when was the fault first detected;

- error resolution description: resolved, pending, under investigation, no further action, unresolvable;
- error code: e.g. A3=printer fault, B2=vdu faults, C2=application system fault;
- error description : a short narrative describing the fault;
- the source of the error;
- initials of those responsible for maintaining the log, closing the log; and
- section responsible for dealing with the problem.

The ability to add an entry to the log should not be restricted, however the ability to update the log should be restricted to authorised personnel. Management should have mechanisms in place to ensure that the problem management mechanism is properly maintained and than outstanding errors are being adequately addressed and resolved.

7.3.7 Network management and control

A range of controls is required where a client uses computer networks . Network managers should ensure that there are appropriate controls to secure data in networks, and that the network is adequately protected from unauthorised access. The controls may include:

- separation of duties between operators and network administrators;
- establishment of responsibility for procedures and management of remote equipment;
- monitoring of network availability and performance. There should be reports and utilities to measure system response time and down time; and
- establishment and monitoring of security controls specific to computer networks.

8 Physical and environmental controls

8.1 Introduction

The objective of physical and environmental controls is to prevent unauthorised access and interference to IT services. In meeting this objective, computer equipment and the information they contain and control should be protected from unauthorised users. They should also be protected from environmental damage, caused by fire, water (either actual water or excess humidity), earthquakes, bush-fires, mud-slides, electrical power surges or powercuts.

According to the Information Systems Audit and Control Association (ISACA) the second most likely cause of errors is natural disasters (user errors being number 1, fraud no 3 and hardware faults no 4).

There are two ways of restricting access to the computer systems, physical access and logical access. This chapter looks at physical access and the protective measures to physically protect a computer system. Logical access is considered in chapter 9.

8.2 Risks associated with poor/absent physical or environmental controls

8.2.1 Physical

- accidental or intentional damage by staff:
  - IT employees;
  - cleaners, security guards;
  - other employees.
- theft of computers or their individual components (computer theft is on the increase and is likely to continue. Consider that, weight for weight, computer chips are worth more than gold and are very attractive to thieves);
- power spike or surges which may cause component damage and the loss or corruption of data;
- bypass of logical access controls: e.g. having physical access to a fileserver can be exploited to bypass logical controls such as passwords; and
- copying or viewing of sensitive or confidential information, e.g. pricing policies, pre-published results, government policies.

8.2.2 Environmental

- fire/water damage (or damage from other natural disasters);
- power: Cuts, leading to loss of data in volatile storage (RAM);

- Spikes :leading to system failures, processing errors;

- failure of equipment due to temperature or humidity extremes (or just outside tolerances of a few degrees);
- bomb damage. terrorism appears to on the increase around the world. Computer centres would be easy to attack and their destruction may have significant repercussions on the government;
- static electricity : can damage delicate electrical components the computer clips (ROM, RAM and processor) are delicate and easily damaged by static electricity shocks;
- others : e.g. lightning strikes.

Some of these risks are also covered in greater depth in the Business continuity planning chapter of this IT controls module.

The financial IS auditor's main concern is that an incident associated with lax physical or environmental controls will increase the risk of either:

- damage to the client's computers and financial data, restricting their ability to record financial transactions and produce a set of auditable financial statements;
- errors in the accounts, caused by fraud or client mistakes.

8.3 Client approach to addressing physical and environmental risks

It is management's responsibility to ensure that adequate internal controls exist to protect the business's assets and resources. To do this, management should carry out a risk assessment. This would involve identifying the threats to the systems, the vulnerability of system components and likely impact of an incident occurring. Management then identifies counter-measure to reduce the level of exposure to an acceptable level. Management must balance the risks identified with the cost of implementing controls.

Some controls would be expensive to implement and would only be justified in a high risk environment. Other controls would be considered to be baseline controls, e.g. door locks and would be found at most clients.

The client's IT security policy should include consideration of physical and environmental risks.

The counter measures, or controls that the client puts in place will vary from one client to another. For example, a large government Department with its own purpose built data centre will usually have a higher degree of controls over its IT facilities than a small organisation using office automation systems such as word processing and spreadsheets.

8.4 Specific physical and environmental controls

8.4.1 Physical control of secure areas

Physical access controls are specifically aimed at ensuring that only those who have been authorised by management have physical access to the computer systems. Physical access security should be based upon the concept of designated perimeters which surround the IT facilities. For example, the client could designate an IT perimeter around the building, around the computer suite, around the printer room etc. The perimeters should be clearly defined and staff should be aware of where the boundaries are.

Access to the client's site and secure areas should be controlled by layers of controls, starting at the perimeter fence and working in through the building's entrance to the computer suite and terminals. Physical controls may be explicit, such as a door lock; or implicit for example an employees job description implies a need to enter the IT operations area.

8.4.2 Administrative controls:

- staff wearing name or identity badges;
- removing access rights of staff who are dismissed.: e.g. the security guards are informed when staff leave, or keys being returned when staff are dismissed. There should be procedures to identify leavers and ensure that their physical access to the building is not allowed;
- visitors : logging of visitors, including who they are, who they work for, who they are visiting, arrival time, exit time. Visitors may be asked to provide some form of identification before entry is allowed, e.g. a driving licence or identity card. Visitors may be required to be escorted at all times;
- unattended office procedures: i.e. what should be done when staff leave their office unattended e.g. then staff go home at night or out to lunch. Measures could include locking their keyboards, putting laptops in locked drawers and locking away floppy disks.
- Locks on doors - physical locks on doors require one of two things to gain access. Either what someone has or what someone knows. Whatever method is used, the "key" to each type of lock need to be tightly controlled, for example who should be given a key or who should be told the keypad combination. Commonly encountered locks include:

    - mechanical key locks : the door keys should be stamped "do not duplicate" and the keys should not indicate the facilities to which they grant access;
    - combination door locks or cipher locks: these are normally keypads with numbered buttons. Authorised staff are given the combination to gain access. Combinations vary from 3-6 numbers and should be changed regularly, or when a member of the IT staff leaves or moves to another part of the organisation;
    - electronic door locks : These normally use plastic cards with an magnetic strip on the back. The magnetic strip is used to hold a special code which is read by a card reader. If the code is correct the locking mechanism releases and allows entry. Electronic door locks offer advantages over manual keys locks as they:
        - can be set up to identify individuals and log their movements;

- restrict access to particular areas of the organisation according to user need (or time of day);
- can be difficult to duplicate, especially if they are smart card with an in-built microchip;
- can be easily controlled from a central console, e.g. if an employee leaves, it would take only a few seconds to disable that users access rights; and
- can be connected to silent alarms which activate in a control room when unauthorised access is attempted.

- biometric door locks :these locks are programmed to recognise the biometric features of authorised users. Biometric features which may be used include handprints, voice patterns, fingerprints, retina scans or a signature. Biometric systems tend to be expensive and are usually only used in very sensitive computer facilities.

Other physical controls include:

- video cameras : video cameras can be located at strategic points to monitor and record entry and exit. If video cameras are monitored 24 hours a day they can act as a preventive control. They can also be a detective control in that they provide a visual log;
- security guards : security guards may be deployed at the entrances to the client's premises. They may be used to check the identity of all those entering the facility. They can also be used to carry out patrols during non-working hours;
- perimeter fences : surrounding the computer installation;
- burglar alarms: these may be useful where to monitor inactive entry points such as fire exits, or when IT facilities are unattended;
- control of out of hours employees : for most clients this include office cleaners , maintenance staff and security guards and sub-contractors. It is not unusual to find that clients have strong controls over staff movements, but weak controls over other out of hours contractors. For example, a security guard may have access to most parts of the client's premises and also be able to come and go out of office hours without being subject to the normal security procedures. There have been many cases where cleaners have not just been cleaners but have had another agenda (e.g press, espionage, theft);
- deadman doors : deadman doors may be found at the entrances to sensitive areas such as the computer room. They consist of two doors, only one of which can be open at any time. They are useful in preventing unauthorised persons from following an authorised person into the facility, i.e. they help prevent piggybacking. Other controls similar to deadman doors are revolving doors and one-person tubes;
- computer locks : some makes of computer have in-built key locks which lock the keyboard or the computer's Input/Output mechanisms to prevent unauthorised. access. The problem with this control is that users frequently loose the keys or leave them in the locks at all times;

Where a high risk of computer theft or vandalism has been identified there are several controls which the client may consider;

- security cabinets : with the increase in chip theft, security product suppliers have produced metal security cabinets. These consist of metal shells which can be attached to a solid surface. The computer is then locked into the metal shell. This makes it more difficult to prise open the computer and remove the chips;
- intelligent water : this consist of water with a unique chemical signature. When the client's premises is broken into an intruder detection system activates and sprays the "intelligent" water from ceiling level sprinkler nozzles. All persons (thieves etc) and equipment coming into contact with the water can then be traced back to the crime scene;
- "fog screens" : these devices activate when an intruder is detected and spray a mist into the room which creates a dense fog. This reduces the visibility to the extent that it is then very difficult for a criminal to see what s(he) is doing.

8.4.3 Environmental controls

Fire prevention, detection and suppression:

These systems are designed to prevent a fire breaking out in then first place and if a fire does occur deal with it in an efficient manner.

Fire prevention controls may include:

- making the IT facilities fire resistant by using fire resistant building materials;
- a no smoking policy in the building or the computer suite;
- a clean computer room, where dust and paper are not allowed to accumulate;
- fire detection controls may include smoke and heat detectors.

Fire suppression controls may include:

- hand held fire extinguishers: care needs to be taken to ensure that the correct extinguisher is on hand. For example, some extinguishers are unsuitable for electrical fires. Portable carbon dioxide or halon (BCF) fire extinguishers are suitable for use on electrical fires. Water extinguishers should be available in or near stores of computer consumables, e.g. printer paper and stationery;
- automatic suppression systems: These systems activate automatically when a fire is detected. They normally sound an audible alarm when activated and begin a timed countdown before the fire suppressant is released. The system should divide the premises into segments or zones. This allows the system to activate only in those areas where a fire has broken out. Fire suppression systems often use either water or halon. Halon is favoured as it does not damage equipment like water and it is less hazardous to health than carbon dioxide extinguishers.

The fire suppression system should be regularly maintained to ensure it is in proper operational condition. The client's premises should also be inspected by the fire department or authorities.

Staff should be trained in the proper use of the fire suppression equipment.

Protection from water damage

Computer equipment (and in particular the electricity which powers the equipment) and water don't mix. Therefore computer facilities should firstly be located in a position where the equipment is less likely to come into contact with water, and secondly if water does manage to get into the computer rooms, its presence is detected.

Water can enter a computer room from a number of sources, including;

- floods;
- leaking roofs;
- burst pipes;
- overflowing sinks, toilets;
- leaking radiators; and
- condensation.

Since water flows under the influence of gravity, the risk of water damage can be reduced by locating the computer facilities at a higher elevation, i.e. not in the basement. It is common for computer facilities to be located on the third to sixth floors of buildings.

Water detectors should be placed under raised floors. They should be connected to visual and audible alarms.

Even where computer facilities are located above ground level, there may still be a risk of water damage from burst pipes or leaking roofs. Flat roofs have a reputation for leaking.

Protection and control of the power supply

The auditor's primary concerns relate to the possible impact that electricity has on the availability of the systems and the integrity of the data processed.

The client's systems should have controls in place to minimise the effect of a power cut or deviations in supply (power spikes or drops in voltage). This is normally achieved through the installation of:

- **electrical surge protectors** : the voltage and frequency of mains power can vary. Computer equipment can be sensitive to theses variations and should be protected from power spikes and drop-offs and frequency variations. Voltage regulators monitor the incoming electricity and moderate it according to system requirements. Electrical surge protectors are commonly built into uninterruptible power supply devices;
- **uninterruptible power supplies** : uninterruptible power supplies (UPS) equipment allows for the continuity of computer processing until the power returns, the back-up generator can be activated or the system can be closed down in a controlled manner.

UPS requirements will vary according to local needs, e.g. the frequency and duration of power outages.

Additional power controls can include:

- **back-up generators**. : back-up generators are normally used when power cuts last for more than a few hours. Two types of generator are available, diesel and gas turbine;
- **alternative power cabling** : in some circumstances clients may feel the need to connect their computer facilities to two electricity substations in the hope that an interruption to one power supply will not affect the other.

Heating, ventilation and air conditioning:

Many of the larger computer, mainframes and minicomputers require a controlled environment in which to operate efficiently. They may require control or both temperature and humidity. Mainframes can generate a significant amount of heat and without proper ventilation there is a risk of equipment failure.

These may be controlled through the operation of air conditioning equipment.

If air conditioning is important to the continued operation of the computer equipment the auditor should review the client's maintenance procedures and contracts.

Maintenance and housekeeping

The client may have controls to ensure that the computers and the areas in which they are located are clean and free from debris (waste paper, dust, smoke, etc).

There may also be polices prohibiting the consumption of food and drinks in the vicinity of the computer equipment. A knocked over cup of coffee can have a significant impact on a computer.

9 Logical access controls

9.1 Introduction

The days when information was written on paper and stored in filing cabinets are, for the most part, in the dim and distant past. Today, the majority of the financial systems encountered by auditors will be computerised.

Clients rely on their computer systems to initiate, record and report financial transactions.

The next issue to consider is how to protect the data and business resources.

Computer systems are such that they cannot easily be controlled by physical access controls such as locked draws and cupboards. This is especially true when a client's computers are connected to local or wide area networks.

For example

A financial system is connected to a wide area network using telephone communication links such as dial up modems. Locks on doors, burglar alarms, security guards etc would not be able to stop someone accessing the computer system across the network. Some other method of protecting the systems and the data they process is required. This is where logical access controls come into play.

Logical access controls are defined as:

"a system of measures and procedures, both within an organisation and in the software products used, aimed at protecting computer resources (data, programs and terminals) against unauthorised access attempts."

There are three basic elements to logical access security.

User identification

This normally involves a user identifying himself/herself to the computer with a user-name or logon id etc.

User authentication

The computer requires confirmation that the user is who s(he) says they are. This is achieved by something the user has or knows. Passwords are a common form of authentication. Other forms of authentication include PIN numbers (used to authenticate yourself after putting your bank card into an ATM), a signature or biometrics such as your hand-print.

Resource protection

Resources are the computers files, directories, peripheral devices. Resource protection is based on the needs of each user. For example, when a user logs in

(identified and authenticated) the computer knows who they are and restricts access to certain files applications or other resources according to their job requirements.

The auditor should bear in mind that some operating systems and associated logical access control options, file parameters etc are very technical in nature. Where the client's systems are technically complex and the auditor does not have a working knowledge of the client's particular systems, the IT auditor may need to obtain additional support and assistance from an IT auditor with the relevant skills and experience.

It is unlikely that an external IT auditor will have a detailed knowledge of more than a few systems (e.g. the more common operating systems such as Unix, Novell and Windows NT).

For example carrying out an audit of an IBM mainframe running MVS. Unless the external IT auditor has prior experience of either operating or auditing such systems, it is unlikely that the auditor would know enough about the system to carry out an in depth technical audit.

When tasked with an in depth review of logical access controls on a complex system the IT auditor may need to call in additional assistance from specialist in that operating environment.

9.2 Risk associated with inadequate logical access controls

The main impacts which could arise from a lack of logical access controls are:

- unauthorised disclosure;
- unauthorised amendment; and
- breach of system integrity.

The possible impact of a breach in a logical access controls is greater where the computers are used to initiate, as well as record transactions. In manual systems, finance staff were careful with cheque books and other financial documents. Where a client has a computerised system the same principles apply and the client should have controls to prevent unauthorised people from gaining access to the electronic financial records and documents (e.g. a computerised payments file prior to its transmission to the bank).

If the client's systems are connected to a wide area network such as the Internet, then the risks are even greater. The nature of electronic records is also such that it may not be apparent that anyone has made an unauthorised amendment.

This should bring home the importance of logical access controls for ensuring the integrity, availability and confidentiality of the client's financial systems.

9.2.1 Attackers

Computer systems may be attacked from several directions. The attacker that first .springs to mind is the computer hacker.

Hackers are normally highly computer literate people who attempt to gain access to a system to prove that they can. They see hacking as a personal challenge. Although their prime intent is just access they may inadvertently cause damage to the systems or data.

Employees : these may be staff from the IT department or normal system users. The auditor should take note of the controls over temporary and part-time staff.

Former employees :former employees, especially those with a grudge may attempt to access the system to carry out some form of revenge.

Outsiders : may include competitors, foreign powers (espionage), organised crime.

Vendors and consultants : These are often the people who put a system in place or those who maintain it.

9.2.2 Consequences of a breach in logical access security

Qualification of audit opinion: As external auditors this is the most obvious concern. The accounts may be un-auditable because of a loss of the financial audit trail, or the accounts may contain material errors due to a loss of data integrity.

Financial loss:. The loss can be direct losses due to fraud, or indirect losses arising from the cost of amending the system and correcting the data.

Legal obligations: The client may have certain legal obligations concerning the storage and disclosure of data, e.g. if there is legislation requiring the client to maintain the confidentiality of any personal data. In a banking environment a loss of integrity could lead to a breach of banking regulations and disciplinary action.

Loss of market share and, or credibility : This is especially important in the financial services sector, e.g. banks and securities and investment bodies. A breach in security can lead to a loss of credibility and eventually a loss of business.

Disruption of business activities. : for example, if a hacker gained access to a computer system and changed all the product dimensions in a manufacturing processing system.

9.3 Resources, files and facilities requiring protection

9.3.1 Data files

These may consist of transaction files or databases. Any files containing masterfile or standing data information should also be protected, e.g. files containing payroll rates, bank account codes system parameters etc. If not protected someone could make unauthorised amendments or even delete the data.

9.3.2 Applications

Unrestricted access increases the risk that the financial applications will be subject to unauthorised amendment leading to fraud, data loss, and corruption. Unauthorised access to the source code of an application could be used to make amendments in the programming

logic., e.g. rounding off payments to the nearest unit (pence, cent etc) and posting the rounded fraction to the programmer's expense repayment account.

Where a system carries out complex calculations it may not be possible to independently check the applications calculations and unauthorised amendments may remain undetected for a considerable time.

9.3.3 Password files

If these files are not adequately protected and anyone can read them there would be little to stop an unauthorised person obtaining the logon identification and password of a privileged system user. Any unauthorised user who obtained the access permissions of a privileged system user would be able to cause considerable damage.

Even where the identifier and password of an ordinary user are obtained , the concept whereby users are held accountable for their actions is bypassed. The unauthorised user could use the "stolen" identification to make amendments which cannot be traced back to the perpetrator.

9.3.4 System software and utilities

These consist of software such as editors, compilers, program debuggers. Access to these should be restricted as these tools could be used to make amendments to data files and application software.

9.3.5 Log files

Log files are used to record the actions of users and hence provide the system administrators and client management with a form of accountability. A system log can record who logged onto the system and what applications, data files or utilities they used whilst logged on. A application log can be used to record changes to financial data (who changed what data, from what to what, and when). If log files are inadequately protected, a hacker, fraudster etc could delete or edit it to hide his/her actions.

9.3.6 Spooled and temporary files.

Spooled and temporary files may be used to store information before it is acted upon. For example when a user initiates a cheque print run, a temporary file containing the cheque details is created. This file is used to print the cheques when the printer is ready. Without adequate protection, someone could edit the file and change payment details before they are sent to the printer.

9.4 Access security framework

It is responsibility of the client's management to ensure that there are adequate controls to address any identified risks to the systems. Management should direct what logical access controls should be in place by firstly establishing a corporate access security policy.

In drawing up a policy management should determine the business requirements for access control and determine the access requirements for each system.

Corporate security policies are normally relatively short documents. They may contain:

- definitions: e.g. what is meant by security and specifically the terms confidentiality, integrity and availability;
- security statements e.g:
  - every system and related files must have an owner and must be classified in terms of the importance of confidentiality, integrity, and availability;
  - access to the information contained in the systems will be granted only on a need to know basis. The need to know will depend upon the function (roles, responsibilities and duties) of each system user and the function of the computer system; and
  - the level of protection will be commensurate with the level of risk and the value of the asset;
- responsibilities : the responsibilities of all users should be defined. This is normally done by grouping users into "normal users", system owner, security management and IS/IT audit.

Detailed logical access controls will be based on the high level statements within the corporate IT security policy.

9.5 Operating system and application access controls

Logical access controls may, and in financial systems usually, exist on two levels, the installation level and the application level. Consequently, access controls may be built into:

- the operating system (or bolt on utilities); and, or
- each application.

The logical access controls at each level are normally controlled by different administrators. Someone in the IT department would be responsible for administering who can log onto the network and once they are logged on what applications and data files they can get access. This person controls access at the installation level.

A separate application administrator would be responsible for administering who can do what in each application.

The system administrator in the IT department would have a better understanding of the operating system and its resources and would know what applications and powerful systems utilities need to be protected. This would allow for the protection of system resources from outsiders, and unauthorised IT staff.

The application administrator would have a better knowledge of the applications and those who use it. This understanding of the application would allow the application administrator to alter access privileges according to the needs of each user. For example, someone with a knowledge of the finance department would know what activities each member of staff requires to carry out their duties effectively. This would ensure that users are only given

access to functions within the application which they require for their job, e.g. the application administrator would know that a purchase order clerk would not need access to the sales system so access to that system would not be permitted. (Application security is also covered in chapter 17).

This approach adds to control in that access security duties are segregated between the system administrator and the application administrator.

9.6 Logical access controls at the installation level

Logical access controls are frequently built into the operating system software by the manufacturer (Unix, Novell, NT). The strength of the access controls varies from one product to another. There are some organisations which carry out independent testing of the security features within operating systems. The criteria for evaluation of "trusted" computer systems viz. CC (Common Criteria), ITSEC (IT Security Evaluation Criteria) and TCSEC (Trusted Computer Security Evaluation Criteria) are described in the IT Security module.

Where operating systems do not have in-built logical access security the client may have installed a separate package. For example, it is common for users of IBM mainframe computer to install access control packages such as RACF or ACF2. There are also propriety security packages availability for microcomputers.

9.6.1 Account Management

The organisation should have a systematic policy for managing information system accounts, including establishing, activating, modifying, reviewing, disabling and removing accounts. This would broadly cover the following activities:

- Identification of account types (individual/ group/ system), and establishment of conditions for group membership.
- Specification of access rights/ privileges on a need-to-know basis;
- Procedures for identification of requests to establish accounts, and approval of such accounts;
- Monitoring of guest/ anonymous accounts, and disabling of unnecessary accounts.
- Notification to account managers of change in IS users' status (transfer / termination etc.)

9.6.2 Logon procedures

Terminal logon procedures are used to gain access to data and applications on computer systems. When the user requires access to the system the logon process activates (e.g. simply by powering up or by clicking on an icon or typing out a logon command). This initiates a logon script. The logon procedures guide users through the steps they must take to identify and to authenticate their identity to the computer. This usually involves users entering their login ID followed by a password.

Login procedures should incorporate the following controls:

- the name of the organisation should not be displayed until after the user has successfully logged on. This limits the clues the system may give an unauthorised user. For example, if a national space research organisation displayed a login message with the name of the organisation, an unauthorised user would have a head-start when attempting to guess passwords. They would try passwords such as nebula, quasar, solar, etc;
- the login should not "welcome" anyone. There is a famous case whereby a hacker gained access to a computer system which had a welcome screen . The hacker escaped prosecution because the welcome screen was deemed to be an invitation to attempt to access the system;
- the login script should not inform the user of success or failure until the whole login process had passed. This ensures that an unauthorised user is not informed of where s(he) went wrong;
- automatic disconnection after a set number of login attempts; and
- any on-screen help facilities should be disabled during the logon process to ensure that unauthorised users do not receive guidance on accessing the system.
- Once users have successfully logged on, the system may be able to display the last login time and date of the user, and details of any unsuccessful login attempts. This should bring any access attempts to the attention of the user. For example, if a user logs onto the system in the morning and a message appears saying last login at 0430 am, s(he) would know that something was wrong.

9.6.3 User identification and authentication

User identification is normally achieved by users entering a login identifier. The client should have a policy for the composition of login identification codes, for example, the first three letters of their surname, their initial and a two digit number.

e.g. Mr James Smith has a login id of SMIJ27.

Whatever policy the client decides to adopt it should ensure that the login ids of each user are unique. Uniqueness is important as it allows for the identification of each person. This in turn aids accountability, especially where the authenticated login ids of users are logged against the activities they perform on the system.

The computer should maintain a list of logon ids for all authorised users.

Other systems may use a token as a form of identification, e.g. a card with a magnetic strip on the back.

9.6.4 Authentication

After a user has identified himself to the computer system the computer has to confirm that that person is who s(he) claims to be. This is known as authentication.

Authentication is achieved by the user knowing something, possessing something or from a comparison of physical characteristics. Authentication factors can generally be classified into three categories:

- Something the user is (e.g. fingerprint, retinal pattern, DNA sequence, voice pattern, signature recognition etc.)
- Something the user has (e.g. ID card, security token, software token or cell phone)
- Something the user knows (e.g. password, pass phrase or PIN)

9.6.4.1 Passwords

To be effective, password controls should address:

- password composition. The client's password policy should prohibit passwords which are based on:
  - family names, addresses, initials (including pets);
  - car registration numbers;
  - telephone numbers ;
  - easy to guess combinations e.g. qwerty;
  - solely alpha or numeric characters. (the more options the harder a password is to guess);
  - dictionary words (words from science fiction television programmes are common);
  - what users can see from the window. (It is reasonably common for users to use a password based on something they can see from their desk, e.g. Compaq 486, or the name of the petrol station across the road).
- minimum length : the more characters the more difficult to guess. However the longer a password must be, the more likely it is that users will forget what theirs is. A minimum of 6 characters is common for financial systems;
- password ageing : i.e. they should expire after a certain number of days (30 -60 days is common). In addition some systems do not allow users to change their passwords immediately after making a change. They must wait a period, e.g. 7 days before they can change the password again;
- password history: some password systems keep a history record of the last few passwords and prevents the user from reusing an old one. This prevents users from recycling a few of their favourite passwords;
- password secrecy : i.e. stipulating that passwords should never be written down or shared with another person. In addition passwords should not appear on the screen when users enter them. The screen should display a series of stars or asterisk e.g. ******;

- initial allocation : there should be initial allocation procedures for adding new users to the system should be in operation. Initial passwords are usually allocated by the system administrator. If the system allows users to change their passwords they should do so at the earliest opportunity. The system may be able to force users to change their password, for example when the system administrator adds a new user, the password life can be set so that it has already expired. When the new user logs on for the first time the system tells him/her that the password was expired and must be changed before any further logons are allowed;
- password encryption. : passwords should be protected to prevent unauthorised disclosure. Encryption is a common method of protecting the data in the password file. If you can see an unencrypted password you will be able to tell what the actual password is. You can then copy it and use it at a later date;

Some systems apply an algorithm to the users password and store the result in a password file. When that user logs on the password they enter is encrypted using the same algorithm and compared to the encrypted password in the password file. If they match access is granted;

Other systems store encrypted passwords in a hidden file which cannot be seen by users. This prevents hackers from obtaining copies of encrypted password files and running programs such as "crack" against it. Crack is a Unix program that encrypts words and compares them to the encrypted passwords. Where matches are found you know what the password is;

- staff leaver passwords: when staff leave the organisation their ids and passwords should be locked. This reduces the risk of a former employee, who may be disgruntled, from accessing the computers. This may require the client setting up procedures whereby the IT administrator is kept informed of staff termination. It is reasonably common for IT to be the last to know then a member of staff has been disciplined; the " but nobody told us to remove his login!" should be avoided;
- vendor and default passwords : when new systems are installed they normally have user accounts set up for the system installation engineers, vendors and consultants. These accounts normally have high access and privilege levels. These accounts should be tightly controlled, and disabled if necessary. For example, accounting packages may have a standard user account to allow system testing. This account may have the ID "test" and an associated password "test";
- user guidance, procedures and awareness : users should be aware of what the client's password policies are. For example they should know that passwords should not be shared or written down. Written procedures may be of benefit to users as they would reduce the likelihood of users making mistakes when they are changing their password etc (e.g. what keys to press and how to think of a hard to guess, yet memorable password).

9.6.4.2 Multifactor authentication

Historically, the majority of access control systems authenticate the user by requiring the input of a password. However, with increasing Internet connectivity and its attendant risks,

strong authentication[1] involves the use of multiple authentication methods to provide more reliable authentication of identity. For example, the US Government defines four levels of authentication from Levels 1 to 4, with Level 1 providing the lowest assurance and Level 4 the highest:

- Level 1 – This provides some assurance that the same claimant is accessing the protected transaction data. It does not require "identity proofing", nor are cryptographic methods required. While plaintext passwords or secrets are not transmitted across a Level 1 network, simple password challenge-response protocols are allowed.
- Level 2 – This provides single factor remote network authentication with identity proofing requirements. Successful authentication requires that the claimant prove, through a secure authentication protocol, that he controls the authentication token.
- Level 3 – This provides multi-factor remote network authentication, with a minimum of two authentication factors, and involved proof of possession of a key or a one-time password through a cryptographic protocol. Successful authentication requires that the claimant prove through a secure authentication protocol that he controls the token, and must first unlock the token with a password or a biometric, or must also use a password in secure authentication protocol, to establish two factor authentication.
- Level 4 – This provides the highest practical remote network authentication assurance and is similar to Level 3, except that only "hard" cryptographic tokens are permitted.

9.6.5 Resource protection

Having access to a computer and being able to log on does not imply that a user can have unrestricted access to all the applications and data files. An additional level of controls is required to restrict users to only those applications, data files or system resources (e.g. invoice printers, cheque printers, backup tape drives) for which they have been granted specific access.

Menu controls can be employed to restrict access to particular users. Menu restrictions can be used to ensure that only those users who should have access to a particular application or data file have such access. Menus controls can be present within the operating system, utility software or applications.

For example, when a sales order clerk logs on, he will be presented with a menu of applications on the system. The option could read as follows:

- Sales system;
- Purchasing system;
- Stock system;
- Personnel system.

[1] As per the US Government's National Information Assurance Glossary, strong authentication is defined as a layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.

The system administrator can set the system up so that the sales clerk only has access to the sales system, the other menu options such as purchase order processing, stock management and personnel would be "greyed" out and hence unavailable.

9.6.6 Securing files and programs

Access to system functions and data should only be granted to authorised users who require access to carry out their jobs. The nature of this access and usage should be specifically authorised by management, taking integrity and confidentiality concerns into account. The client may rely on application owners to approved access to their applications before access is granted. Application owners are normally the senior user of an application and they are given the responsibility for ensuring that the application continues to meet business objectives. For example, the owner of a financial accounting application is normally the head accountant, the owner of a personnel system is normally the personnel manager. Their approval would have to be sought before any new users could be granted menu access to their applications.

Controls may include:

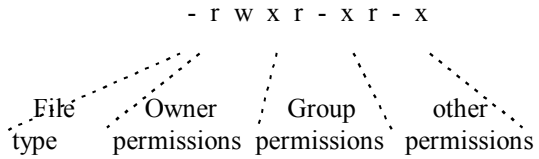
- authorisation to use specific functions (e.g., utilities, menu items and their underlying programs, etc.);
- the ability to 'contain' users within their group of authorised functions, as well as to restrict functions by user, time, and resources. Users may be restricted to certain defined menus. When someone logs on to the system they are automatically placed in a controlled environment and are presented with their menu options. Any attempts to access other parts of the system (e.g. the operating system command line prompt, for example, by pressing the escape key) would result in the system logging the user off;
- denial of operating system prompt, e.g. on a DOS system the C:\ prompt and on a UNIX system the $ or # prompt. Restricting access should reduce the risk of a user loading and, or running unauthorised applications or system utilities.

File permissions : the ability to restrict access to data including differentiation between enquiry and updating or modifying of data. Each resource on the system may be assigned access privileges. When a users attempts to access a resource their permissions are checked against the file's permissions. If the user has the right privilege levels s(he) may be able to use the file or resource.

Common file/resource attributes are:

- read;
- write;
- create;
- update;
- delete;
- execute; and
- copy.

For example, on a UNIX system file, permissions may be displayed as follows:



File types include

:- is a plain file
c is a character device (e.g. a printer)
d is a directory
b is a block device (e.g. a disk or tape)

File permission include

r read permission : where a user can open a file and read its contents
w write permission : where a user can overwrite a file or modify the contents of an existing file
x execute permission : allows a users to run a file or application

When reviewing file permission controls the auditor should check that the following supplementary controls are in operation:

- ensure that access permissions are consistent with authorised requirements and that access in one area or to one function does not circumvent authorised restrictions in another. E.g. having read permission of a directory may override specific permissions allocated to files within that directory; and
- special restrictions of the ability to add, delete, or modify menu items, programs, or utilities. This ability is usually restricted to the system administrator.

Access permissions should be reviewed and kept up to date.

9.6.7 Other logical access controls

Limiting the number of concurrent sessions. This means that when a user is logged onto the system they cannot then go to another terminal and log on again. This reduces the risk of an unauthorised user gaining access to the system. If the legitimate user is logged on, the impostor cannot gain access. If the impostor is logged on and the legitimate user attempts to gain access but is prevented, the user is informed of the problem and corrective action can then be taken.

Limits on working hours: some operating systems (e.g. Novell and Windows NT) can restrict users access to predefined time periods. E.g. if management believed that no member of finance would have need to gain access to the system during the night (e.g. 9 p.m. to 6 am) the system could be configured so that they cannot log on during those specified hours.

Restricted sign on attempts : This involves setting limits on the number of unsuccessful password attempts a user can have before their ability to log on is locked. Setting an upper limit on the number of unsuccessful attempts reduces the risk of someone guessing passwords. Once the limit is reached, a system can lock a user's id for a set period, e.g. 30 minutes or keep the id locked until released by the system's administrator.

Automatic terminal time-out : unattended terminals may be exploited to gain unauthorised access to a computer system. Some systems can be configured to log users out after a set period if no user activity is detected. Alternatively a screen saver may activate which requires the user to re-enter their logon password to free the screen (e.g. Windows 95 and Windows NT).

Terminal specific access : It may be desirable to restrict access to certain applications to specified terminals. For example the client may wish to configure a system such that access to a payroll application can only be gained from a terminal in the personnel department.

9.7 Logging

The controls mentioned so far have been preventive in nature, i.e. they are designed to ensure that unauthorised persons are prevented from gaining access to the computer systems.

The next line of controls involves the detection of unauthorised access attempts and activities. This is normally achieved through the logging of events in an audit log.

There are two types of audit log commonly used by computer systems, the security audit log and the transaction audit log.

The security audit log may be used to record a wide variety of information on user activities.

The following are examples on commonly logged security events:

- access failures : when users have unsuccessfully tried to log on or an attempt was made to access a protected file of directory; and
- use of system utilities and applications. recorded detail could include which application was accessed, by whom and when.

The auditor should be aware that logging every security event would take up a significant amount of system resources and lead to system degradation. In addition, the client is unlikely to spend time reviewing huge log files. The client should strike a balance between the significant activities which are logged and the importance or sensitivity of the systems.

The audit logs should be protected to ensure that they can't be over-written or deleted by someone attempting to covering their tracks.

Where a large amount of data is written to a log file, the client may use exception reporting tools which scan the log files and highlight those events requiring additional attention.

The second type of log, the transaction audit log is use to record the passage of transactions as they are processed by the system. Transaction logs are covered in chapter 17, application security.

10 Change management

10.1 Introduction

This chapter concentrates on the role and requirements of the external financial auditor. Guidance on role of the internal auditor and the performance auditor is provided in other INTOSAI IT modules, "the audit of developing systems" and "performance audit of IT" respectively.

Even when the system development process has been completed and the new system is accepted, it is likely that it will have to be changed, maintained, or altered during its lifecycle. This change process may have an impact on the existing controls and may affect the underlying functionality of the system. If the auditor intends to rely on the system to any extent to provide audit evidence, a review of the change controls is required. Change controls are needed to gain assurance that the systems continue to do what they are supposed to do and the controls continue to operate as intended.

Change in the context of this chapter refers to changes to both hardware and software. Hardware includes the computers, peripherals and networks. Software includes both the system software (operating system and any utilities) and individual applications.

The scale of change can vary considerably, from adjusting a system's internal clock, to installing a new release of an application or operating system. The effect that a change has on the operation of the system may be out of proportion to the size or scale of the change made.

With computer systems the saying "a butterfly flaps its wings in Peru and it snows in Japan" can be said to apply to computer system changes.

10.2 Reasons for system changes

After systems are implemented the system maintenance phase begins. Systems rarely remain the same for long. Even on the day systems go live there are invariably users who are not satisfied with the systems and submit request for changes (RFC) to be made.

Changes may be requested for the following reasons:

- to enhance functionality : everyday system users may not be content with the functionality of the system. This could include discontentment with the screens they have, the system response time. Users may also identify bugs in programs which cause the system to produce erroneous results;
- to make systems operations easier, more efficient: this category includes the tape/disk operators, the Helpdesk manager, the database administrator and network management personnel;
- capacity planning: the system may require additional resources or increased capacity components e.g. a more powerful CPU to cope with increased processing demand, or additional disk drives as the existing drives fill up;

- problem rectification : helpdesk incidents leading to the identification of problems: each incident recorded on the Helpdesk will contribute to the identification of underlying problems. If the problems are significant enough a request for change may be produced by the Helpdesk function;
- to improve security : IT security personnel : identified weaknesses in system security may result in requests for change which should improve security;
- routine updates : system developers may update and improve the system software. They may also request changes when software suppliers "insist" that the client runs the current version of their software; or
- changes in requirements : changes in legislation, business requirements or business direction may require the financial system to be amended.

10.3 Risks associated with inadequate change controls

Change controls are put in place to ensure that all changes to systems configurations are authorised, tested, documented, controlled, the systems operate as intended and that there is an adequate audit trail of changes.

Conversely the risks associated with inadequate change controls are:

- unauthorised changes : accidental or deliberate but unauthorised changes to the systems. For example, if there inadequate controls application programmers could make unauthorised amendments to programs in the live environment;
- implementation problems: for example where the change is not in time for business requirements, e.g. annual tax rates;
- erroneous processing , reporting : systems which do not process as intended. This could lead to erroneous payments, misleading reports, miss-postings of transactions and ultimately qualified accounts;
- user dissatisfaction : systems which users are not happy with: this could lead to data entry errors, staff morale problems, a loss of productivity, union actions;
- maintenance difficulties : poor quality systems which are difficult or expensive to maintain (e.g. due to a lack of system documentation). Where there are inadequate controls over changes there could be multiple changes to the system so that nobody is sure which versions of software, or modules are being used in the live environment. Nobody would know which bugs had been fixed, or what parameters have been altered in different versions;
- use of unauthorised hardware and software : systems (hardware and software) in use which are not authorised. This could lead to incompatibility between different parts of the system, or breach of copyright legislation; and
- problems with emergency changes : uncontrolled emergency changes to programs in the live environment leading to data loss and corruption of files.

10.4 Change control procedures

The client's procedures to control changes should include;

- procedures for management authorisation;
- thorough testing before amended software is used in the live environment;
- management review of the effects of any changes;
- maintenance of adequate records;
- the preparation of fallback plans (just in case anything goes wrong); and
- the establishment of procedures for making emergency changes.

There should be procedures for recording all requests for change (RFC), preferably on standard proformas and/or data input screens. The requests for changes should be logged and given a unique chronological reference number. All RFCs should be allocated a priority rating to indicate the urgency with which the change should be considered and acted upon. The task of determining change priority is normally the responsibility of a change control board or IT steering committee. The change board and steering committee make their views known via an individual given the role of the change manager. The priority of changes is determined by assessing the cost of the change and impact on the business and its resources.

The following chart provides an example of typical change control categories.

Change categorisation

Change Category	Description and impact	Examples of this type of categorisation
E	Emergency changes	Complete system failure Business critical functions unavailable
1	Potential impact on all users of a system	Replace a system Install a new version of the operating system
2	Potential impact on all users of a service or application	Install a new version of an application
3	Potential impact on some users of a service	Reorganise a database correct an error
4	Minor changes requiring the rebooting of the system	configuration changes (adding new system components) Adjusting the system clock
5	Minor changes	Changing network definitions initialising a new hard disk.

Ideally changes to systems components (both hardware and software) should not be carried out until authorisation has been given by the system owner (i.e. the user with overall responsibility for the application and its data files) or user representatives, the programming team leader and the change board (if the client uses a change board). The decision on whether a change should go ahead should consider several factors including:

- the potential impact on the IT systems and services to users (capacity, security, system response times, reliability);
- the effect of not implementing the change (the do nothing approach);
- the resources required to implement the change (costs, people); and
- future resource requirements if the change goes ahead.

If the change board or authorised user has approved a change the change should be scheduled to be carried out. Authorised RFCs should be passed to the relevant technical staff (programmers, operations, network technicians etc) for the change to be made.

Where changes are made to applications, the programmers will request a copy of the current source code. In larger IT departments there may be a specific change control section which controls movement of programming code between the live, development and test environment. Access to the program code should be restricted to authorised change control personnel.

Modifications should be made to a copy of the source code in a controlled development environment, since amending the original could cause problems if the changes were found not to work. The client would have no unamended programs to fall back to if things went wrong.

Once the programmers are content with the amendments they have made, and they have carried out any of their own unit or system testing, the amended software is moved, (by the change control personnel) to a test environment.

All changes should be tested to the satisfaction of users. Alternatively the testing may be carried out by independent personnel responsible for accepting all application revisions. The client should retain documentation of the testing carried out and the results produced.

On completion of program amendment and testing, the update and transfer of the amended and tested software should be carried out a third party, not by the programmer. It is a golden rule that system development staff (programmers and analysts) should not have access to the programs in the live environment. Details of the transfer should be recorded and reviewed by management.

Once changes are made to software, there may be a need to update documentation. There should be procedures to ensure that there is an adequate cross-reference between software amendments and updated documentation. This should provide an audit trail.

After a predefined period the change should be reviewed to determine if:

- the change has achieved the planned results;
- users are content with the amended product;

- there have been any unforeseen problems or unexpected side effects; and
- the resources required to implement and operate the amended system were as planned.

Emergency changes

In certain circumstances it will be necessary for emergency changes to be a carried out. These changes cannot wait to go through the normal change control procedures and must be implemented with minimum delay. For example, if the month end payroll run is about to be made and a programming error causes the application to freeze. Client management cannot wait the usual time it takes to go through the normal change control procedures, since employees need to be paid on time. This is where emergency change control procedures would be used.

The client should acknowledge that such circumstances do arise and that they should be addressed by appropriate emergency change control procedures.

The nature of emergency changes results in reduced time for making the and testing the change. Where emergency change procedures exist the auditor should check that they are reasonable and include some form of control e.g.:

- emergency approval by a member of staff with the appropriate authority;
- audit trail : to provides a record of all the changes that have been made;
- retrospective approval from change board, system owner;
- retrospective testing of the change; and
- documentation update.

Programmers will be under pressure to get the system operating again in the minimum time. Therefore, emergency changes are usually associated with a higher risk of errors and programming mistakes.

Version control

Each generation of software is given a version number. For example the first release is normally known as version 1.0. If minor amendments are made, the next version would be version 1.1. If a major change was then made to the software the next version would be version 2.0 and so on.

Version control procedures are important as they should ensure that the client operates using the correct version of software. Problems may arise if different parts of the organisation are using different software versions which process transactions in a different may, or have different pre-programmed standing data.

Once software has been accepted and released into the live environment it should be “locked” or “frozen”, i.e. no further changes should be made to that version. That version is placed in the production library and should not be changed. If the software, version X requires changing a copy of code would be worked upon and this would be known as version X+1 or version X. 1.

Once the next version of the software is ready for release into the live environment, the “old” copy of the software should be archived.

The increase in distributed computing has increased the need for version control procedures. Distributed computing has also made version control more difficult to control and manage.

Exercise on version control

Sequence of events

Date	**Description**
1 January 1997	Version 1.0 is built and moved to the test environment.
1 June 1997	Version 1.0 is successfully tested and implemented in the live environment. Version 2 is built and moved to the test environment where testing begins.
1 August 1997	A "bug" is identified in Version 1.0 and must be resolved quickly. The user cannot wait until Version 2.0 is ready for live use. A quick amendment is made to a copy of Version 1.0. and the resulting version 1.1 begins testing. Version 2.0 is modified during testing .
1 September 1997	Version 1.1 is successfully tested and implemented in the live environment. Version 1.0 is archived and retained in case reversion is required. Version 2.0 continues testing.
10 September	A serious software error is found in Version 1.1 and management decides to revert to version 1.0. Version 1.1. is archived.
1 October 1997	Version 2.0 passes testing and is implemented in the live environment. Version 1.0. is archived. Version 3.0 is built and begins testing
1 November 1997	Version 3.0 passes testing and is moved to the live environment. Version 2.0 is archived.
1 December 1997	Version 4.0 begins testing

10.5 Control of special amendment facilities

There may be occasions when the client needs to make changes to programs and data using non standard utilities or system development tools. The most common reason for such occurrences is when the programs or operators have corrupted live data. It may be uneconomic or too slow to write a program to correct the errors. Users may require changes to be made immediately.

To meet this need some computer system manufacturers provide special amendment facilities which allow a programmer to change data. The scope for error and fraud increases where there facilities exist.

Examples of special amendment facilities:

- ICL : Change Data; Patch Block; On-line Edit
- IBM : IEBCOPY; AMASPZAP; IEHPROGM
- DOS : DEBUG

The auditor should determine whether special amendment facilities are available and if so what controls there are to restrict the use of these programs. Controls may include:

- restrictions on access to these facilities, e.g. by passwords;
- controls to prevent the copying or re-naming of the facilities;
- use of the facilities should require high level approval;
- all use should be documented and the documentation retained;
- management should review the documentation to ensure that only changes they have authorised have been made; and
- management should monitor the use of these facilities to detect misuse, e.g. by reviewing relevant operating system logs.

10.6 Automated change control systems

Some clients may make use of automated software control applications to manage and control programs.

These applications can assist the client in a number of ways. They can:

- carry out program maintenance functions by assigning version numbers to different versions of software;
- provide access controls through security features such as password access to segregate duties between programmers and operations;
- provide a backup facility to automatically back-up software; and

- provide an audit trail of changes made to software. This information can be presented in management reports.

Examples of this type of software are CA-PANVALET and CA-Librarian.

11 Network controls and use of the Internet

11.1 Introduction

The majority of systems encountered in medium to large scale organisations use either local or wide area networks to connect users. The use of networks is increasing and bringing clients the following benefits:

- the ability to share data;
- to use and share other peripherals, e.g. printer sharing;
- to leave system administration to a central team;
- allow users to send almost instantaneous messages, e.g. e-mail; and
- allow users to access the systems from remote locations.

Opening up systems and connecting them to networks is not without its risks. The network should be controlled such that only authorised users can gain access.

Control of networks is not just about logical access security and keeping out hackers. Networks are primarily used to transmit data. When data is transmitted it may be lost, corrupted or intercepted. There should be controls to reduce all these risks.

The scale of networks is also growing. Recent years have seen the growth of the Internet, the huge global network which allows million of users to interact over communications links. The Internet has brought to light several issues which need to be addressed before deciding to connect up.

The details of networks and the related controls are elaborated in the module on “IT Security”.

12 Third party service providers

12.1 Introduction

The term 'third party service suppliers' is used whenever an IT service or IT related service is provided by an organisation which is independent of the client.

Facilities management is when a third party takes over the day to day running of a client's computer systems. The applications and the equipment remain the property of the client. The third party suppliers simply provides the staff to run and maintain the hardware and software.

Outsourcing ; is when a client contracts with a third party for the provision of complete IT services. The third party owns the hardware and provides the staff and accommodation.

Market testing : this term encompasses both facilities management and outsourcing. It is used to describe the process by which internal services such as IT are subject to open competition. The name for this process may vary from country to country, e.g. in Australia they call the process CTC (competitive tendering and contracting).

Market testing is frequently associate with terms such as "right sizing" and "downsizing". These terms refer to the process by which IT functions are reduced in size (staff numbers, equipment) and cost, theoretically to provide a better match with the rest of the business.

All or just a part of an IT department may be subject to market testing. Some organisations market test the provision of maintenance (hardware and software). Others may outsource all development work, whilst some may decide to just outsource computer operations. It is common for organisations to use third party suppliers for PC support.

Even where the client decides to keep IT services in-house, the decision was likely to take account of recommendations from other third party suppliers, i.e. consultants.

12.2 Benefits of using third party service suppliers

The use of third party services is not a new development. Computer bureaux have been around for many years. Even in the early years of computing when large computers were very expensive rather than just reasonably expensive, some organisations bought time on large computers to process particular jobs.

However, the proportion of services supplied by third parties has continued to increase. The main reasons for this development are:

- cost : IT service suppliers can often provide services cheaper than in-house sources. The large IT service suppliers may benefit from economies of scale and can supply services cheaper;

- cashflow constraints : where equipment needs replacing. Rather than spending a large amount of cash up front to replace the equipment, outsourcing the IT

function will result in a smaller initial outlay. For example instead of paying $1million for a new mainframe outsourcing may cost $250k per annum for the next 5 years;

- staffing : clients may not wish to undertake staff recruitment, training and retention;

- scheduling : dealing with peaks an troughs in the workload. Third part suppliers may be able to divert resources from other operations when one of their clients has a peak workload;

- provision of specialists : the organisation may only requires the services of a specialist for a short period of time. If the IT services were provided in-house, keeping such a specialist on the payroll would be very expensive, considering they would only be required occasionally;

- experience and expertise : alternative solutions : the IT service suppliers are likely to have a wide experience of many different industrial sectors and many organisations. They may be able to provide suggestions and improvements in the IT services which would not have been thought about if the service had remained in-house;

- accountability: when a service is provided by a third party, then that third party assumes responsibility for delivering the service to agreed standards at the agreed price. The supplier is responsible for resolving problems. This makes it easier to assign responsibility and accountability of IT services; and

- faster implementation of new systems : new systems are likely to be developed and implemented on time because service providers are likely to have more experienced systems development personnel, more resources to tackle problems when they arise.

In certain countries, it is compulsory to market test certain public sector IT services. For example, in the UK the central Government requires local government to market test IT services. If third party services can provide a cheaper, and or better service they are awarded the contract.

12.3 Possible problems associated with third party service provision

Purchasing IT services from a third party service provider is not without its risks. As far as the external financial auditor is concerned the risks may need to be examined from two angles, firstly, where the client has decided to purchase IT services from a third party ; and secondly, where the client is an IT service provider.

The areas the auditor should examine are different in each case. Where the client purchases services, the IT auditor would most likely review the contract and ascertain how management administers the contract.

Where the client is a service provider the IT auditor will need to clearly establish the aims of the review. If the auditor is merely providing an opinion on the client's financial statements then the auditor would not need to look at the systems which provide the services to other business. Instead the auditor would concentrate on the service suppliers own accounting systems. However if the auditor was tasked with providing a review of the services provided by the supplier, for example to provide an independent assessment of the controls for the service suppliers clients then a complete review of all the systems would be required. The auditor would then review the service supplier's logical, physical access controls, change management controls etc.

The rest of this chapter concentrates on clients who purchase third party IT services and what the key issues are when this occurs.

12.3.1 External audit access rights

The external auditor may need access to the service provider's systems to verify that they process the client's financial information accurately and that there are no significant factors which would affect the auditor assessment of fraud or material errors. If IT services were provided in-house by the client, this assessment would normally be based on a review of the client's systems of internal control.

Irrespective of whether the transaction recording is carried out in house or by external providers the external auditor would need to understand the systems of internal control and the flow of transactions through the system.

It is usually the case that the third party service provider provides IT services to many organisations. Where this is the case, it would be impractical for the external auditors of each organisation being audited to descend upon the service supplier and review their systems. In these situations it is common for the service provider's own external auditors to provide their clients' auditors with certificates. The certificates would include an opinion based on their independent assessment of the service provider's systems of internal control.

If the external auditor decides that direct access to the third party suppliers is essential to the audit, the auditor should ensure that the client inserts an appropriate audit access clause into the contract before it is agreed and signed.

Note : If the external auditor also has a responsibility for reviewing economy, efficiency and effectiveness (performance audit), the contract with the service supplier should include clauses which allow for external audit access rights. Access to performance audit purposes is also covered in the INTOSAI IT audit training module "performance audit".

The following is an example of a clause which may be used as a basis for an access clause in a contract.

"*For the purpose of examination and certification of XXXX's (the client's) accounts, the YYYYY (SAI) may examine such documents as he may reasonably require which are owned, held or otherwise within the control of ZZZZZ (the service provider) and may require ZZZZZ to produce such oral evidence or written explanations as he considers necessary."*

The SAI should only examine records which relate to the client being audited and not on the supplier's own financial affairs.

12.3.2 Errors in processing

To ensure that the processing carried out by the supplier is accurate and complete the client may need to have procedures for reconciling data sent to the service supplier with data received back after processing has been completed.

Some organisations may have read only on-line access to the service providers systems. This allows the client, and the auditor, to trace transactions through the service provider's systems.

Even if the service supplier found errors in its processing of the client's data, there is a risk that they would not report the problem to the client, i.e. they may try to cover things up and carry out their own fixes before the client notices (the conflict of interest scenario).

12.3.3 Control over system security

Both the client and the external auditor would be concerned that the service supplier maintains an appropriate level of security over the client's data. There is a risk that the security standards and procedures within the service provider are below the level adopted by the client. To reduce this risk the client should include security clauses within the contract which place a responsibility on the contractor to ensure that the security of the client's data is maintained to a specified standard.

12.3.4 Dependence on the third party service supplier

When a client hands over the provision of its IT services to a third party, there is a risk that it may become dependant upon that same supplier for many years to come, perhaps even beyond the period of the contract.

Typically, when IT services are taken on by a third party, the client loses the majority of its own in-house IT expertise. Frequently, staff are made redundant or are transferred to the service supplier. This makes going back to the days when the service were provided internally an unlikely possibility. Once outsourced the IT functions are likely to stay outsourced.

In addition, the expertise in dealing with the client's systems will be gained by the employees of the service supplier. This makes it difficult to move away from that supplier once the contract ends. The learning curve for a replacement supplier may be steep .i.e. it may take months for a new contractor to reach the same level of proficiency.

To reduce the potential reliance on the existing service supplier, the contract should include clauses which allow for a hand-over period after contracts are re-let. This would ease the transition from one supplier to another.

The client should also bear in mind questions such as what would happen if the service supplier went bankrupt or was forced to terminate business, e.g. due to legal problem. There would be little to gain from suing a company already in liquidation.

The external auditor would be concerned in such a case because if the client places complete reliance on the service supplier and the supplier went out of business, then the client would not be able to continue processing in a satisfactory manner. The most likely outcome would be incomplete or inaccurate financial statements and a qualified opinion.

12.3.5 Loss of flexibility

As part of the tendering and contract award process, the client agrees with the supplier, what services are to be provided. Once the contract is signed, there may be no provision for the client to request changes to be made. The supplier could take the opinion that:

> "if it is not in the contract we are not doing it."

This problem may be particularly applicable in the public sector where business needs change whenever there is a change in Government or government policy.

For example, an election may bring in new politicians with new goals. These goals are translated into business objectives and ultimately into new demands on the service provider. The client may need to ask the question " what can we do if the supplier is unwilling to change to meet the new demands?"

This situation can cause the external auditor problems. For example if the client switches its IT service supplier mid-way through a financial accounting period. The external auditor would have two systems to review and output of two systems to audit.

To reduce the risk of this problem occurring, the client should include change clauses within the contract. The clause should allow for changes to be made in line with possible changes to business objectives.

12.3.6 Cost of change

We have already considered the impact of a service supplier refusing to change a system or service. The IT service provider may have no contractual obligation to change a system to meet new business requirements. Where this is the case the only way of ensuring that the supplier complies is to agree an additional fee. Such fees are usually large.

The external financial auditor may not be too concerned if the client has to pay more as long as the cost is reflected in the accounts. However, if the external auditor also has a duty to report on performance issues s(he) may feel the need to report on the contract and any additional payments made by the client.

The client should take precautions to reduce the chance of being forced to pay large amounts for any changes they may require at a later date. These could include clauses in the contract which would specify agreed rates for any changes in the systems, service targets or variations for changes in the volume of transaction processing.

12.3.7 Loss of in-house IT specialists and expertise

Where services are supplied by third parties the client no longer has a need to employ IT specialists. This results in drop in the technical expertise of the remaining client IT staff. This

in turn reduces the ability of the client to deal with unforeseen technical problems. The client would also be at a disadvantage when discussing technical matters with the service supplier.

The loss of technical expertise will probably make bringing the IT services back in-house an unlikely proposition. Rebuilding an in-house team to take over the provision of IT services would be difficult to achieve. Once outsourced IT services will probably remain outsourced.

12.3.8 Staff Resistance

When existing IT services are market tested, there is a risk that staff will loose their jobs. Even where an in-house bid is accepted, the process could lead to changes in working hours, job conditions or rates of pay. In addition, employees may feel that they are doing a good job and that they are being unfairly treated.

These changes can lead to staff resentment, loss of morale and a drop in productivity and performance. The external auditor would be concerned that staff resentment does not lead to unauthorised activities or behaviour, e.g. fraud and sabotage.

12.4 Contracts

It is important that the client draws up a formal contract with any third party service supplier. The contract should be reviewed by a lawyer experienced in these types of contract to ensure that both parties are protected against unreasonable clauses.

Contract with third party service providers should include:

- duration of the contract;
- termination rights;
- audit access;
- limitation of liability;
- indemnities;
- intellectual property rights;
- ownership of data;
- handover arrangements at end/termination of contract;
- security standards;
- service levels;
- charges, costs and invoicing; and
- change control.

The contracts specify the details of the services to be provided and should be reviewed by the auditor.

12.4.1 Duration of the contract

The contract should specify how long it lasts for, including the start date and the end date.

The auditor should check that the duration of the contract is not excessive. The client should not tie themselves into a very long term contract, especially where the client operates in a changing environment. Changing a contract mid-term can be difficult if not expensive.

The contract may also include an extension clause, e.g. if both parties agree the contract may be extended for another 1-2 years. These clauses can help to reduce costs as the client will not have to go through the re-tendering process as often.

12.4.2 Termination rights

The contract should include each parties' termination rights. Sub-clauses could include what will happen to the data, equipment, software, and what if any penalty clauses will be applicable. The period of notice should also be stated.

Unless the contract specifies reasonable termination options, there is a risk that the service supplier could terminate the contract prematurely and leave the client without the ability to process. This would have a knock-on impact on the client's ability to prepare year end accounts.

12.4.3 Audit access

Unless the contract specifies that the service supplier will provide access to the client's auditors there will be no automatic rights of audit access.

The auditor should determine what access rights are required to enable the auditor to carry out his/her duties and ensure that theses rights are included within the client's contract with the service provider.

Access rights may also include granting access to the client's internal auditors. If this is the case, the external auditor may be able to place reliance on the internal auditor's work.

12.4.4 Limitation of liability

This clause deals with the liability of both parties in the event of one party experiencing a loss due to the action of the other. The clause may specify any limits on consequential losses, e.g. a limit of £1 Million could be set on consequential damages (to cover lost business, fines or penalties) which the client incurred because the service provider failed to provide the contractual services.

12.4.5 Indemnities

Indemnity clauses are designed to protect one party from third party claims. It is usual practice for the service supplier to indemnify the client against claims.

Example of indemnity clauses include, the service supplier indemnifying, or covering the client for claims where a third party claims breach of copyright or intellectual property rights. Indemnity clauses may protect the client against claims of negligence or injury to the service suppliers employees whilst processing the client's transactions, e.g. if a service supplier gets his fingers damaged in a printer whilst printing the client's invoices.

12.4.6 Intellectual property rights

This clause also relates to copyright. The contract may include clauses which specify who has the rights to software developed or maintained by the service supplier on the client's behalf.

The ownership of intellectual property is important, especially when the contract terminates and the client chooses a new service supplier.

12.4.7 Ownership of data

This is similar to the ownership of intellectual property rights except that it relates to the data processed on the client's' behalf. The contract should make it clear that the ownership of the data remains with the client and not the service provider.

12.4.8 Handover arrangements

The contract should specify what the arrangements are when the contract comes to an end and a new service supplier takes over processing. The contract may need to specify a handover period in which the new supplier's employees get to know the software and processing methods.

The old supplier should be contracted to provide assistance during the handover period to ensure that processing continues in an uninterrupted manner.

12.4.9 Security standards

The contract may specify that the service supplier adheres to specified security standards. The standards may be national standards such as the UK's British Standard for Information Security (BS7799) or the client's own security standards. Where the client adheres to pre-defined standards, it is more likely that the IT auditor will be able to place some reliance on the IT controls.

The service supplier's security standards should be reviewed to determine if that there are appropriate controls to ensure the integrity, availability and confidentiality of the data.

There should be a mechanism for providing assurance that the security standards are being adhered to. This assurance may come from the service supplier's own independent auditor, from the client's internal auditors; or directly from the external auditor's own reviews.

The auditor should also consider what security arrangements there are for protecting data in transit between the service supplier and the client. For example, if the client prepares a payments file and sends it to the service supplier on a floppy disk, there should be controls to ensure that the disk cannot be tampered with without detection.

Where the service provider processes data on the client's behalf the provider also assumes responsibility for ensuring that the data is adequately backed up. The auditor should check that the contract requires regular backups to be made.

12.4.10 Service levels

The contract should include a schedule describing the levels and standards of service to be expected. The schedule should cover the service the supplier has agreed to provide. Delivery targets should be set in terms of:

- quantity :e.g. how many transactions will be processed, reports etc the services provider will produce;
- quality : e.g. processing time, availability of services, standard of output, assistance to be provided, response time.

12.4.11 Contract monitoring

Once the contract is in place the client should establish monitoring procedures to ensure that the agreed services are being satisfactorily delivered.

There should be regular meetings between representative of the service provider and client management to discuss the services being delivered and resolve any disputes.

12.4.12 Charges, costs and invoicing

The contract should include a schedule detailing the cost of the contract, together with charges for any additional services. Long term contracts may also include a provision for increasing prices e.g. in line with inflation.

The frequency of invoicing should also be included within the contract, e.g. annual, quarterly or monthly invoicing. These may also be clauses specifying payment terms, e.g. payments should be made within 30 days of an invoice being received.

12.4.13 Change control

The longer a contract is the more likely that the systems will have to be changed during the life of the contract. The contract should include principles by which either party can propose changes.

Where changes are permitted, the contract should allow for changes to be tested before use in the live environment.

13 End user computing controls

13.1 What is end user computing?

The term end user computing is an imprecise term. In essence it refers to the situation where users have intelligent computers on their desktops (i.e. computers with their own CPU processing capabilities), together with applications which allow them to develop their own processing, and reporting systems.

End user computing has given users greater control over the processing and presentation of their data. Conversely, end user computing has reduced the control exercised by central IT departments.

There are four common types of end user computing. These are:

- personal computers;

  The use of personal computers accounts for the biggest rise in end user computing. In 1995 there were estimated to be 120 million IBM PC compatible computers world-wide. The days are approaching when it will be considered normal for all users to have a personal computer on their desks. Personal computers are mainly used for office automation (word-processors and spreadsheets), database interrogation, E-mail and group working. They are also used to access the central systems, e.g. the finance system.

- report writers and extraction software (e.g. SQL);
- executive information systems (primarily by senior management); and
- system generation tools, e.g. CASE tools and fourth generation languages.

13.2 Risks associated with end user computing

From the beginning, developments in end user computing environments has been uncontrolled. Users do not adopt the same standards or good practices that their colleagues in the IT department use.

This uncontrolled environment can, and has led to a waste of time, effort and money for the client. The fact that end user computing has been so uncontrolled also causes the auditor concerns , especially where financial transactions are processed by end users.

The majority of end user computing problems and risks have arisen from the historical absence of controls. Users see their desktop computer as their territories over which they exercise their own controls and do what they like. This has led to several specific risks.

13.2.1 Systems development

IT departments usually have staff experienced and trained in the development of computer systems. They are trained and have experience of:

- what standards the systems should to be developed to;

- what documentation is required;
- what controls should be built into the new system; and
- what testing is necessary to ensure that the system does what it is supposed to do.

End user computing has permitted end users to develop their own applications without assistance from central IT departments. The end users developing their own systems do so without the relevant skills and training.

When you have systems being developed in the absence of standards, by non-experienced or trained staff you invariably get problems. Typically these include:

- unreliable systems which do not process data in the way intended, e.g. the underlying logic of the applications has not been thought through or coded correctly;
- systems which do not include basic data integrity, input, processing or output controls. For example financial accounting systems which accept single sided double entries, resulting in unbalanced trial balances;
- systems which are untested and unpredictable. For example, if the system has not been tested to ensure that it can deal with incorrect data input it may crash or hang when such data is entered by a user;
- systems which are not documented. This makes it difficult to maintain the system in the longer term. IT auditors have frequently heard clients tell them that an application was developed by an employee five years ago and since that person left no-one has been able to find any documentation to enable them to understand exactly how it works;
- systems which have been subjected to uncontrolled change. End users have a habit of diving in whenever that find a problem in their own applications. They tend not to follow the same change control procedures as used in IT departments. This leads to changes which are poorly thought out and programmed. These changes may have a detrimental impact on the system. For example, a user may change a formula in a table, and unknown to him/her it has an unplanned knock on effect elsewhere;
- incompatibility and fragmentation of information: the systems purchased by end users may be incompatible with the corporate systems. This makes on-line sharing of data difficult to achieve. Data on end user systems may not be up to date and include the latest amendments to the data on the central system.

13.2.2 Duplication of effort.

When end users take responsibility for their applications they tend not to consult with the rest of the organisation and rarely co-ordinate their efforts. This leads to duplication of effort as two different parts of an organisation attempt to develop an end user application to solve the same problem. Additional problems arise when they discover the duplication and nobody wants to shelve their project. Alternatively both may be developed, doubling the maintenance effort required to keep them up and running. As the systems were developed by different users it is possible that they produce different answers to the same problem.

13.2.3 Data inconsistencies

Data may also be inconsistent from one user department to another. With traditional management and reporting hierarchies, updated information has to go up one branch of a management hierarchy before being disseminated back down another.

Data inconsistencies are likely to be greater where the client uses a distributed system.

Data inconsistencies can cause the auditor problems if different parts of an organisation use different standing or masterfile data in their calculations, e.g. pay rates for sub-contract staff, or unit costs for sales invoices or overhead apportionment rates for the calculation of full costs.

13.2.4 Increased use of resources and costs

Experience has shown that end user computing has increased the cost of most organisations' IT services. The increased costs are not just from putting personal computers on users desks. Costs have increased due to increased training requirements, greater demands on help-desks. There are also additional hidden costs such as users spending more time trying to solve their own and their colleagues IT problems.

End user systems have a tendency to be less efficient in their use of resources, e.g. CPU time, networking and printing resources. For example report writers require significant amounts of processing power, which can slow down the rest of a system. In some organisation users are not allowed to run their reports during normal working hours. Instead the reports have to be run overnight.

13.2.5 Erasure of central information.

End users may download data from the central system for examination or processing with their own end user developed applications. Problems can arise where the flow of data is two way, i.e. after the user has processed the data it is then uploaded back into the central system, overwriting the original files. This increases the risk of information needed for the audit being overwritten by incorrect information. In addition the audit trail may be obscured or lost when users overwrite the original data files.

13.2.6 Compliance with legislation

Without prompting from the central IT department, end users are less likely to be aware of legislation associated with the use of computers, the storage of personal information, privacy, or copyright.

When users have personal computers on their desks there is a temptation to copy and use illegal software. The attitude "nobody will know if I use this software" is reasonably common amongst PC users.

An organisation or even individual employees are unlikely to escape prosecution by using the excuse that "I didn't know what the law required, nobody told me."

13.2.7 Loss of data

IT departments usually recognise the importance or regularly backing up data to ensure that if a problem or disaster occurs then the systems can be rebuilt, together with the data. Unfortunately, the same is not true in end user computing environments.

Another problem relating to the loss of data is the increase in computer theft. Computers, and especially the latest high tech personal computers, are valuable pieces of equipment. Their high value has made them targets of computer thieves. Whole computers may be stolen, together with the information they hold.

The increasing portability of end user computing in the form of laptop and notebooks has created a new risk. Their inherent portability increases the risk of a whole computer being lost or stolen e.g. when there computers are left on trains or stolen from hotel rooms, luggage racks or airports.

13.2.8 Logical and physical access security

The majority of personal computers use either the DOS, Windows 3.x, Windows 95, OS/2 or Macintosh operating systems. These operating systems are designed for single users and consequently have little in the way of logical access controls to restrict access to unauthorised users.

It is reasonably easy to bypass any of the security controls which these operating systems use. Anyone with a reasonable knowledge of the operating system would be able to access any data file or application desired.

Physical access to desk-top computers is normally less controlled. An organisation's mainframe and minicomputers are usually located in a controlled environment with access restricted by locked doors, keypads combination locks and CCTV. The same is rarely true of end user computers. These are normally located on top of desks in the normal office environment.

Having physical access to a PC can be exploited to bypass the simpler logical access controls, e.g. the basic Windows type user passwords. Data may also be stored on floppy disks which can easily be copied. The data may also be edited or deleted by unauthorised users.

13.3 Computer viruses

Computer virus are in effect small programs which are designed to replicate and spread from computer to computer by attaching themselves to either another program or the boot sector of a disk.

Computer viruses activate and replicate when the file they are attached to is run or when a computer boots from an infected disk. Once activated, viruses can remain active in the computer's memory waiting for something to infect.

Viruses and other forms of malware, and their associated controls are discussed in detail in the module on "IT Security".

13.4 End user computing controls

Where organisation make extensive use of end user computing, the auditor is likely to find that the general control environment will be weak. This may be due to insufficient staff to segregate duties, lack of training for computer users, inadequate resources or a lack of management commitment to establish standards and sound controls.

This inherent lack of general controls may increase the risk of errors and fraud. Where organisations use end user computing and the auditor is required to assess the possibility of relying on the computer controls, s(he) is more likely to look for the existence of management and administrative controls, rather than detailed technical controls within the computers and applications.

One of the biggest problems encountered by clients when dealing with end user computing controls is ensuring that all the relevant staff are aware of the policies, standards and working practices that must be adopted. This may be overcome through a comprehensive education program for system users. Information can be passed through a combination of newsletters, bulletin boards and formal training.

13.4.1 Systems development controls

These may include establishing system development policies and standards for end user developed applications. The level of formalisation may be dependant upon the criticality of the application to the business. For example where an application is important its development should be formalised and tightly controlled. On the other hand where an application is not important and only used locally by a few employees, the development process would not have to be tightly controlled.

Development standards would ensure that the initial development of , and subsequent changes to, important applications are subject to approval, and that they are documented and adequately tested.

The problems associated with incompatible systems can be reduced if the client has policies and procedures for the acquisition of hardware and software. The policies may also include procedures for making asset purchases and recording asset locations in a register.

13.4.2 Duplication of effort

Users should have a mechanism by which they can communicate their efforts to others in an organisation. This could be done by arranging regular meetings between middle and lower level management. Local developments in IT systems could be one of the discussion items on the agenda.

13.4.3 Data inconsistencies

Where updated information is important, the client should have a system to ensure that all those using the data have an up to date copy. This problem is normally solved by holding the data on a central database. The applications developed by end users could use the information in the database instead of relying on outdated information in local data files.

The client could also have procedural controls to ensure that the most up to date information is used. For example a check list could be drawn up to prompt users into using the latest information.

Where users can access the information contained in a central database, access permission should be established so that only authorised users can amend the central data.

13.4.4 Legislation

The client should establish policies to ensure that end users are aware of, and comply with relevant legislation. The awareness programme may cover:

- software theft : i.e. the unauthorised copying of an organisation's software or data for personal use or gain;
- compliance with health and safety legislation;
- the use of pirated and illegal software; and
- the collection, use and storage of personal information (privacy legislation).

13.4.5 Data loss

Where important applications or data are stored on end user computers, the client should establish controls to ensure that the organisation would not be adversely affected by a disaster affecting those computers.

Control procedures could include:

- requiring users to back up their applications, data and documentation on a regular basis and storing the back-ups in a secure location (off-site if required). The frequency of backups should be dependant upon how important the data is, the timeliness of the data and how many transactions are processed in a given period; and
- storing data on a fileserver instead of on local hard or floppy disks. The fileservers are normally administered by the IT department and should have established procedures for backing up the data on a regular basis.

13.4.6 Logical and physical access

Users should be encouraged to adopt at least basic logical access security precautions on their standalone personal computer, e.g. setting the BIOS password.

If possible data should be stored on network fileserver. In general the network operating system will provide a degree of protection against unauthorised access via the network.

Where a client uses portable computers there should be policies which require them to be placed in a secure environment overnight, e.g. in a locked drawer or cupboard. Even SAI's with 24 hour security have experienced lost or stolen laptop computers.

Where the client considers risks to be particularly high consideration should be given to installing security software on end user computers. These should have more robust logical access controls and may encrypt sensitive data.

13.4.7 End user support

End user computing is on the increase and is likely to become more significant in the future. The client should have established a framework to provide users with support.

End user support is normally provided via a help-desk function. The help-desk acts as the interface between the IT professionals in the IT department and the end users. User request for help should be passed on to the IT specialist with the appropriate skill and knowledge.

14 Introduction to application controls

14.1 What are application controls?

Computerised financial controls extend beyond the general IT environment. We also need to look at the controls within individual applications.

In the past, when an auditor was confronted with a manual system, the auditor would look for the presence of manual controls which ensure that individual transactions are initiated, authorised, accurately processed and manually recorded in the accounting ledgers. The same is true when the client uses computerised applications, i.e. the auditor should look for controls within a application which ensure that transactions are properly initiated, authorised, processed and recorded.

When a client installs a computerised accounting system the underlying control objectives and concepts remain the same. All the computer does is modify the nature of risks. Computerised financial systems can also incorporate automated controls which don't require human intervention. For example, in a manual system a finance clerk would have to manually check the account code on a journal existed. In a computerised application the system would automatically check that the account code keyed in by the user referred to a valid account code. Where it didn't an error message would be produced and the transaction could not be processed until a valid account code was entered.

The trend is towards more automated financial systems where transactions are entered into the system at an early stage. In the past the transactions were initiated on paper, authorised on paper and they would only get recorded on the computer system at a late stage, e.g. just before a payment was made. In today's systems, transactions can be automatically generated or they may be entered onto in the system directly by a user, without the user first having to complete a manual form, e.g. a paper purchase order.

Application controls do not only refer to those controls which are built into an application which ensure that valid transactions, and only valid transactions are processed and recorded completely and accurately in the accounting records. Application controls can also refer to the manual controls which operate in proximity to an application, for example a data entry clerk requires a data input form to be signed before it is entered onto the system. Application controls can be categorised as follows:

- file integrity controls;
- application security controls;
- data input controls;
- processing controls;
- output controls; and
- masterfile and standing data controls.

In some situations the auditor may need to consider network and communications controls. The auditor may need to identify any controls which exist to ensure that data transferral is complete and accurate.

14.2 Application users, administrators and owners

There are normally three types of user associated with financial applications.

14.2.1 Application owner

Firstly, there is the application owner. Application owners are normally a senior user. They are frequently drawn from the highest level of management personnel who use the system on a regular basis. For example the owner of a financial accounting application is normally the head of finance. The owner of a stock and stores system would be the warehouse manager, and the owner of a personnel system would be the personnel manager.

The application owner in effect has overall responsibility for the strategic contribution the system makes to business objectives. For example the finance manager in charge of the accounting system would be responsible for ensuring that the organisation's transactions were being recorded completely and accurately and that the system was producing the required output, e.g. management reports on sales, spend vs. budget etc.

The auditor should note that the concept of an application owner is not always apparent to the client. Therefore when the auditor wants to find out who the owner is, it may be necessary to ask questions such has "who has overall responsibility to the Board (senior management) for ensuring that that accounting system operates as intended?"

The application owner also has responsibility for ensuring that the system is used by the right people and that it continues to operate as intended. The application owner is normally a busy member of staff and hence is unlikely to have sufficient have time to look after and administer the system on a day to day basis.

Hence, the auditor will frequently find that the day to day administration of the system is delegated to an application or systems administrator.

14.2.2 Application administrator

This person would be responsible to the system owner. Typical tasks carried out by a systems administrator include:

- maintaining a list of authorised application users;
- adding and removing users from the application's security profiles;
- ensuring that the IT department has backed up the data according to back-up policies;
- resolving queries from application users;
- identifying, monitoring and reporting significant problems to the application owner and IT department;
- holding and distributing application documentation; and

- liaison : liaising with the IT department on system performance, e.g. storage requirements, response times. The administrator would also liaise with other application administrators and the software suppliers.

14.2.3 Ordinary system users

These are the day to day users of an application. They are given access to parts of the system they require to do their jobs. Their training on the system is limited. to the user functions needed for their jobs.

Essentially they have to make sure that they know how the use the parts of the system they are authorised to use. They have little knowledge of systems administration duties.

14.3 Application types

Applications are normally categorised according to the way data is entered and available to users. The main categories are:

14.3.1 Batch data entry systems

Batch data entry systems are normally associated with older financial systems. Transactions are normally passed, by users, to a central IT or finance data input section, where they are batched up and entered onto the computer in batches.

14.3.2 Batch data entry with on line enquiry

Transactions are entered in batches as before, but users can make enquiries on individual transactions as they are entered. However, the effect of the new transactions on balances, account totals, summary figures etc. is not calculated until the entire batch has been input and the batch processing cycle completed.

14.3.3 Batch processing with on line enquiry and update

Users enter transactions at workstations. They can amend erroneous transaction data on screen. The user sees what appears to be an updated transaction record. This is because the transaction the user enter updates a copy of the master file. However, the real copy of the masterfile is not updated until a later time, e.g. overnight updating of the masterfiles.

14.3.4 Real time systems

Real time systems are the latest development in computerised financial applications. Users can enter transaction at a workstation and see an immediate effect on the account balances, i.e. the accounts are updated whenever a user enters a transaction. Real time systems allow users to correct errors immediately and improve the timeliness of management information. However they don't include the traditional controls such as batch totals.

14.4 External audit reliance on application controls

During preliminary planning the auditor should gain an understanding of the client's systems sufficient to determine whether it would be possible to rely on the systems of internal control to gain audit assurance on the accuracy of the client's financial statements.

Where the systems of financial control appear to be sufficiently robust the auditor may then test the controls. Depending upon the number of control failures, the auditor may place audit reliance on the controls and reduce the amount of subsequent substantive testing that must be carried out.

14.4.1 Compliance test programmes

To place reliance on a client's controls the auditor should develop a compliance test programme. These programmes should include the following information:

- a description of the control that is to be tested;
- the evidence that we expect to obtain to satisfy ourselves that the control has operated;
- the extent of planned testing, including sample sizes;
- what will constitute a control failure; and
- how many such failures can be tolerated before the auditor cannot rely their operation to reduce errors.

Testing controls is achieved by gaining evidence that a control has operated. For example if a computer enforces segregation of duties between various finance function the auditor may check the access control lists and the user permissions on those lists. Alternatively, if the computer has automated controls to ensure that purchase order clerks can only order goods from a predefined list of approved products from approved suppliers (regularity assurance), the auditor may check the access controls to the approved products list, together with a sample of new additions to the list.

Evidence that the computer controls have operated will normally be obtained from a combination of observation, enquiry, examination and sampling. The auditor may also be able to use computer assisted audit techniques to assist in the examination of controls. For example, the auditor could download the audit log file and write a routine to extract unauthorised access attempts. The auditor could follow these up to ensure the proper procedures were followed.

14.4.2 Problems with placing reliance on computerised controls

- A problem with testing computerised controls is that they are often built into an application and they may not provide a history of their operation. In manual systems when a check was carried out by a supervisor or another member of staff, a piece of paper such as an invoice or a goods received note would be signed. The auditor would take the signature as evidence that the control has operated. With computerised systems the control may take the form of the supervisor signing an electronic goods receipt note directly on a computer screen. Evidence that the person electronically signed the electronic document would be obtained from testing the access controls to the good receipt approval screens.

- The spans of computerised controls are often limited. For example, they cover just one small stage within the processing lifecycle of a transaction, e.g. the data entry phase. There are many other stages in the processing cycle where things could go wrong and where additional controls testing would be required. Auditors normally prefer to place reliance on controls with a wide span of influence, e.g. bank reconciliations.
- Auditors are often reluctant to place reliance on computerised controls because of the fear of hackers and computer literate fraudsters. Auditor fear that these people can get around many of the automated controls in financial systems. If the auditor places reliance on a control and it subsequently turns out that they were easily bypassed by a computer literate thief then the auditor would feel very uncomfortable.
- Another problem associated with testing computer controls is that they are preventive in nature, i.e. they check data automatically when a user attempts to enter it and reject erroneous transactions. By their nature, auditors are more reluctant to place reliance on preventive controls. They ask themselves questions such as do we know that the control was working at the time, since no errors were discovered and recorded. This problem can be addressed by the auditor actually testing a control during the accounting period. For example, the auditor would visit the client during the year and attempt to input transactions which the systems controls, if operating correctly would prevent. Auditors should remember to get the client's approval before doing this as any erroneous transactions which bypass the controls will have to be identified and reversed at a later date.

14.4.3 Amount of controls testing required

The next question the auditor asks is how to gain the required (planned) audit assurance. This decision is likely to affect the level of controls testing required. When determining how much controls testing is necessary, the auditor should base any decisions on a combination of professional audit judgement and statistical modelling. The factors affecting the auditor's judgement include:

- the frequency of a control : for example, if the auditor plans to place reliance on monthly reconciliations, the control could be tested 12 times in an accounting period. Where controls are frequent they may need to be tested more often;
- degree of reliance on the control : If the auditor intends to place significant reliance on the control or the auditor has assessed that the control mitigates a particular risk in another part of the system, the auditor will need to carry out more testing;
- evidence: the amount of testing may be affected by the evidence available that the control operated as intended. If direct evidence is not available, the auditor may need to carry out more controls testing. As explained earlier many computer controls do not produce direct evidence that they operated and therefore the auditor may need to gain indirect evidence of its operation;
- continuous operation of the control : the auditor will need to determine if the control operated during the whole accounting period. This will require evidence and possible visits to the client at various intervals during the year; and

- importance of the control : the audit should consider the importance or sensitiveness of the transactions the controls are applied to. If the transactions are particularly sensitive the auditor may need to carry out more in depth controls testing.

Where the auditor plans to test controls which are performed on many transaction the auditor will need to determine a sample size. The sample sizes will be largely dependant upon statistical calculations and any audit assurance models the SAI has adopted. The sample sizes will also be dependent upon the auditor's judgement. Any judgement decisions will be affected by the factors described above.

15 Application security

15.1 Relationship between general security controls and application security controls

This chapter considers the physical controls within the finance and the logical access controls designed into individual applications.

The physical and logical access issues considered previously concentrated on what was done in the IT department. This chapter looks at what is done within the users' own departments, e.g. finance , personnel etc. Hence, when attempting to find out about the security controls within an application the IT auditor would need to ask the application administrator within the user department.

Many of the principles in this chapter remain the same as those covered previously and there is a degree of repetition, for example the principle of restricting user access according to their needs.

15.2 Purpose of applications security controls

Application security controls are designed to:

- ensure the integrity of transaction and standing data by allowing only authorised users to access specific application functions and data;
- enforce separation of duties by allocating different privilege levels and menus to individual users; and
- make users accountable for their actions by logging their identifiers against their actions.

As mentioned before, security is all about identifying and authenticating users, protection resources (in this case the financial data and the organisations money), logging and accountability.

The security administrator within the IT department should have ensured that these controls exist at the operating system level. The application administrator would ensure that there are appropriate access and security controls within their applications.

For example, the security administrator in the IT department would ensure that only authorised employees would be able to log on to the network. S(he) would also ensure that only authorised members of the finance department would have access to the directory which held the accounting application.

The application administrator would then deal with the next level of security and ensure that only finance department staff can access the application. In addition, once finance staff have gained access the administrator could then ensure that they are only allowed access to certain modules, e.g. the sales module, the purchasing module or the fixed assets module, provided

that they have been granted permission to use those modules. The application administrator may even be able to control what a finance user can do within each module.

15.3 Commonly encountered application access controls

The extent and number of controls will vary from client to client . The auditor should use judgement when assessing the application controls and should be careful when putting forwards recommendations for improvements. It may be difficult and or costly to bolt on any controls recommended by the auditor.

In addition many clients use off the shelf financial applications with standard access control mechanisms. Where this is the case the auditor should find out what access controls are available and determine whether the client has configured them properly to derive maximum benefit.

15.3.1 Application log-on screens and password controls

When users select the accounting system option from the operating system menu, they "load" the application. The application immediately asks them who they are and what are their passwords. Users are normally required to enter a short ID code followed by their password. This process identifies and authenticates the finance system's users.

As with logon procedures at the operating system level the auditor should review the application's ID and password policies and procedures and controls. For example the policies on password composition, the use of unique ID codes, password ageing policies, allowing users to change their passwords.

The log-on controls built into applications may vary considerably from very good to non existent. Even where an application has good basic password controls, much will depend on how the client implements the access controls. For example the application may have the ability to force users to change their passwords, however if the client does not activate this option it is of no benefit.

Unfortunately the log-on controls within many financial applications are weak. The application may only be able to handle passwords of up to 5 characters in length, there are frequently no password ageing controls, no automated controls over password composition, no facilities for users to change their passwords (i.e. passwords are allocated by the application administrator).

The auditor should check that the application administrator has adopted and makes use of manual procedures to keep password access files and log-on procedures up to date. For example, maintaining contact with the personnel and the IT department to identify starters, leavers and those staff who move from one part of the business to another (e.g. to and from finance). This should enable the application administrator to ensure that only current, authorised users are able to log-on to their application.

Application administrators may not be as conversant with good security practices as the security administrators in the IT department. For example, they are more likely to forget to

disable the guest accounts which are used when a system is set up by a supplier or visitor accounts for temporary staff.

15.3.2 Resource protection

Once users have navigated the log-on screen and successfully gained access to the application they may then be confronted with a menu screen which contains the names of the application modules.

Access to modules may be restricted using an application's access control list or matrix.

Draw the following matrix on the whiteboard as an example of an application access control list.

Name (ID) \	Module		
	Sales	Purchase	Fixed Assets
M.Smith	N	Y	N
C.Henman	Y	N	N
G.Chivers	N	N	Y

Financial applications may have facilities to control access to function within modules. A common way of doing this is to either:

1. for each authorised module user, specify which permissions are granted or disallowed.

2. for each job function e.g. sales clerk, sales supervisor, cashier, etc, specify what functions are permitted. Individual users are then assigned one or more job functions. This method is preferred because it makes the job of the system administrator easier.

15.3.3 Logging and accountability

This is the third area of application security which an IT auditor should review. The basic principle is that users should be held accountable for their actions. Where users can be held to account, they are less likely to make errors (if the error can be traced back to you, it is likely that more care will be taken).or carry out unauthorised activities.

In the past, when manual systems were dominant, user identification and accountability could be achieved by users physically approving (signing, initialling or stamping)financial stationery, e.g. purchase orders, goods received notes, cheques etc. In an increasing number of today's modern computerised accounting system the number of manual forms and paper based financial stationery has declined. There has been an increase in both direct computer input and the use of electronic documents (e.g. EDI).

Where transactions are processed by a computer, applications may produce an electronic audit log. Logs are used to record transaction details such as:

- what transaction was entered (details of account codes, amounts);

- who entered the transaction;
- when was the transaction entered; and
- amendment details (who changed what, when?)

Where an application can produce a transaction audit log the auditor should review what the log has been set up to record.

A large amount of information can be written to an application audit log. The auditor should assess whether too much or too little information is logged. If too much is logged the system's performance is likely to deteriorate. If too little is recorded it may not be possible to find out enough about users and transactions when errors, fraud or other unauthorised activities occur.

The audit log acts as a detective control and is only of use if it cannot be altered or deleted by somebody trying to cover up details of their unauthorised activities. To ensure that the log is safe from unauthorised editing or deletion, the auditor should review access permissions to the log. Normal users should not be able to create edit or delete the audit log. The log may be protected by placing it in a protected directory. Access to the directory would be restricted to a few users (e.g. the application administrator).

Note : directory permissions are likely to be controlled by the IT department rather than the application administrator.

Another way of protecting the audit log would be to write it to a WORM drive.

Some applications may be able to encrypt the audit log. This would make it difficult for an unauthorised user to identify which parts of the log need to be amended to hide their activities.

16 Input, processing and output controls

16.1 Introduction

This chapter considers the controls which are applied, either manually by application users, or automatically by a computer system, to an organisation's financial transactions.

The overall objective of a system of control over any accounting system is to ensure the completeness, accuracy and validity of the accounting records. It should be borne in mind that the objectives of control will be exactly the same for all accounting systems, from simple manual operations to complex real-time database systems. However, the methods of achieving the desired degree of control will vary according to individual circumstances.

Irrespective of whether a financial system is manual or computer-based system, the validity of entries is best ensured by some method of authorisation.

The auditor can place greater reliance on the authorisation of the output from a system than can be placed on the authorisation of input, as this achieves the authorisation of what is actually processed rather than the authorisation of what should be processed.

The financial statements are the product of an accounting system and the main control objectives will be satisfied if procedures are in place to exercise control over the completeness and accuracy of:

- input into the system : this will involve reviewing the procedures and controls which ensure that data input is authorised, complete, not a duplicate, accurate and timely;

- the processing of this input : i.e. the controls which ensure that the correct application and data files are used, all the data is processed, postings are to the correct accounting codes and that the right files have been updated; and

- the output produced by the system : i.e. the controls which ensure that all the output is produced as expected, it is complete and it is sent to the right destination in a timely manner.

It is the client's responsibility to ensure that the application controls are appropriate. As an IT auditor, it is up to us to point out to the client where weaknesses exist. The IT auditor may or may not provide recommendations for improving control (depending upon the remit of the auditor).

An important point to remember is that there are costs associated with implementing controls. Costs can be identified in terms of staff time, processing capacity and efficiency. The client's management will need to consider these costs in the context of the risk given the specific circumstances of the system and the client.

When reviewing a client's input, processing and output controls the auditor should determine if the client has carried out any risk assessment to determine if the controls in place are adequate and cost effective.

Ideally, the auditor responsible for auditing the client's financial statements would be able to review both the manual and computerised systems. However, from experience, it is probable that the financial auditor will lack an appropriate level of IT audit skills and experience and will therefore request the assistance of an IT auditor when reviewing the IT controls. Where this is the case and the IT auditor is asked to assist in the reviewing the client's systems, both auditors should work together and maintain a dialogue to keep each other informed of their findings. This allows both the financial and IT auditor to gain an understanding of the whole system and the overall controls framework in operation. The auditor will then be better placed to evaluate the overall controls environment, including the existence of control weaknesses and the existence of mitigating controls.

16.2 Understanding and documenting an application and its internal controls

International auditing standards state that the financial auditor should obtain an understanding of the client's systems of internal control. This will involve reviewing the client's financial system and documenting:

- the transaction processing system : including how transactions are initiated and how they flow through the client's accounting system. For example, the auditor should find out where source documents are initiated, authorised, processed and recorded; and
- the controls which the client applies to the transactions as they enter, pass through, and exit the financial systems.

To assist the auditor in gaining an understanding of the client's systems, the auditor should find out what potentially useful documentation the client has. These may include:

- flowcharts;
- data flow diagrams;
- user manuals (manufacturer supplied);
- input forms (purchase orders, invoices, goods received notes etc.);
- desk instructions; and
- system reports.

The client's accounting system may produce many reports and various types of output information. It is likely that many of the client's standard reports will be of little audit interest, for example management accounting reports on sales per department, costs per square foot etc.

The auditor should seek to identify those reports which may be of use. The client may have a list of the standard system reports together with a record of any customised user defined reports.

Chapter 5 covered how to document an accounting system, including the three commonly used methods, i.e. flowcharts, narratives and internal control questionnaires. The auditor may use a combination of all three to gain an understanding of, and document, the client's systems.

16.3 Input controls

Input controls should ensure that:

- all transactions are entered accurately;
- all transactions are entered;
- all transactions are valid;
- all transactions have been authorised;
- all transactions have been entered in the correct accounting period; and
- all transactions have been posted to the correct account code.

The auditor should bear in mind that input controls extend beyond just entering data into a computer system and pulling off reports at the other end. The auditor should consider other aspects of application security, such as how the system restricts access to only authorised users. The auditor should also review manual or administrative controls such as segregation of duties within the client's finance department, the delegation of responsibilities, and the custody of :assets, input documents, physical accounting records and financial stationery.

Where a client uses computerised input controls, the financial auditor may be able to gain assurance from their operation. If the auditor decides to adopt a controls reliant audit approach the auditor must test the controls. This may require the auditor to carry out a review of : the system development process; the system testing programme and results thereof; the change control procedures; and the controls in operation.

16.3.1 Authorisation of input

The client should have procedures and controls in place to ensure that all transactions are authorised before being entered into the computer system. From the external auditor's point of view authorisation controls reduce the risk of fraudulent, or irregular transactions. The client also gains better control of resources.

Traditionally manual systems have used a manual form of transaction authorisation. Even where financial systems are computerised many clients continue to use manual authorisation controls such as a signature or the initials of a member of staff with the required level of delegated responsibility. Some organisation may use an authorising stamp instead of a signature.

Computerised financial applications may be able to permit client staff to enter and authorise transactions directly in the system. This can be achieved by setting up password access controls to data input devices and data entry permissions, e.g. data input screens. Menu and data access permissions were covered in chapter 17, Application security.

The authorisation for low value, routine transactions may sometimes be in the form of standing authorisation, e.g. a purchase clerk may have standing authority to enter transactions for utility expenses such as electricity and telephone charges up to a pre-set limit.

For example, a finance clerk is tasked with entering transactions into the accounting system. The access permissions can be set so that the clerk can enter the transaction details. However s(he) cannot authorise the transaction because s(he) does not have the required access permissions to complete the data authorisation screen. The transaction is sent electronically to the budget holder who approves it on screen (they can authorise the transactions because they have the right permissions).

Financial applications may be able to check that a transaction has been approved by a person with the appropriate level of authority by checking their log-in ID against a predefined transaction approvals list.

Management review is another control which the client can use to check that transactions were authorised. The system may be able to display a list of all the transactions (on paper printout or on screen). The manager or supervisor may review the list and may select a sample of transaction to check for proper authorisation.

To place reliance on the automated controls the auditor would need to determine that the appropriate levels of authority have been set up and that they have been working for the whole accounting period. This would involve:

- looking at access matrices;
- obtaining printout of user permissions;
- reviewing audit logs of changes in permissions;
- interviewing users; and
- testing the controls during the year.

16.3.2 Completeness of input data

As part of a financial statement audit, the auditor must determine if the accounting records are complete and that there are no material omissions. To do this the auditor should review the controls which ensure that transactions input is complete, i.e. that transactions have not gone missing.

The completeness of transaction input can be ensured by a variety of controls. These include:

- manual procedures e.g. keeping a log of transactions which users send for input. The data input staff in the finance department may expect a regular flow or pattern of transactions from user departments. Where a batch of input documents is expected but not received or a batch number appears to be missing, follow up action should be taken to identify the missing transactions;
- the use of pre-numbered data input forms. These may be sequentially numbered. When a number is found to be missing the finance staff can investigate any disappearances. Alternatively the input transactions may be sent on sequentially numbered batch forms from user departments;

- use of batch totals : In a traditional batch input system, all data is presented to the system in batches and incomplete batches are detected and exception reports are produced; and
- establishing a routine or expectation of data input. E.g. if data entry staff expect to receive input documents from all 10 departments each Friday and they only receive 9 sets, they would chase up the missing set of input documents.

A batch is a collection of input documents which are treated as one group. The existence of batches is useful in establishing controls to ensure the completeness of input of data to the system. The total of individual transactions should agree to a manually calculated total recorded for input on a batch header document.

A batch system require transactions to be entered in batches. If a batch is incomplete, for example if a transaction is removed, the system would reject the batch on data input because the batch total calculated by the computer would not match the total calculated by the whoever prepared the batch and completed the batch header.

Batch totals should be recorded at the earliest possible point in the processing cycle and totals agreed from update reports back to this original record, i.e. the first batch total acts as a reference to check back to as the transactions are processed by the system.

Control must be exercised by the users to ensure that all batches are processed as well as to ensure that the correct value is accepted for each batch. It is therefore essential that a complete record of all batches sent for processing is maintained. This is usually a log book completed by the computer operators and reviewed and signed by a supervisor.

When batches are prepared and sent for data entry, they are accompanied by a batch header document. Typically a batch header will contain the following information:

- the batch number and date;
- batch control totals; and
- document counts.

Even where batch systems are not used, the client may be able to rely on simple record counts. Whilst record counts do not check that the transaction contains the correct data, they can provide some assurance that transactions have not gone missing.

Applications may also have in-built controls to ensure that all the key transaction information has been entered before the transaction can be posted to the accounts. For example if the finance user does not input data in a key field such as amount the transaction would be rejected by the system.

16.3.3 Data input validation

Financial applications may have in-built controls which automatically check that data input is accurate and valid. Validation may also be achieved by manual procedures such as double checking input documents or review by a supervisor.

The accuracy of data input to a system can be controlled by imposing a number of computerised validity checks on the data presented to the system.

Automated validation checks should be sufficient to ensure that all data accepted into the system is capable of acceptance by all subsequent processes, including acceptance into other systems where there is an automatic transfer of data. Acceptability is particularly important where feeder systems are used. For example the output from a standalone payroll system may provide the input for a general ledger system.

Validation checks can reduce the risk of an application crashing because of logic errors arising when attempting to process input data with values outside pre-defined limits.

For example, the trainees may have heard about the year 2000 problem and the risk that systems will crash when the year goes from 99 to 00. Some applications will crash as 00 is numerically before 99 even though it refers to the following year. A data validation check may be used to deal with this problem.

There are many types of programmed application control which an IT auditor may encounter. For example: format checks, validity checks, range checks, limit checks, check digits, compatibility checks etc.

Format checks

Format checks are carried out to ensure that the data entered conforms to a pre-defined format. For example a particular field may accept a specific combination of alpha numeric characters. Format checks are often applied to fields such as:

Amounts : where only numeric characters would be accepted, e.g. prices of goods or service, or the number of hours worked by employees.

Dates : where a date has to be in DD/MM/YY order as opposed to MM/DD/YY order. Date formats may be important as they may be used to determine year end debtors figure in the accounts. For example does 11/12/96 mean the 11th December 1996 or 12th November 1996. The answer may depend which country the software was developed in.

Account codes : account codes may have to be a numeric value, e.g. 668531. If a data entry clerk in the finance department entered 668S31 the system would detect that the account code was invalid.

Range and limit checks

Range and limits checks are used where a field is pre-programmed to only accept data which is within a specified range. The system may be set to accept an upper and a lower value. If only an upper boundary is set then the control is a limit check.

Limit checks are frequently used to prevent large errors occurring. For example a limit could be set on the numbers of hours en employee can work in a week. If the limit was set to 80 hours and a user incorrectly entered 800 the system would reject the transaction and display an error message.

Similarly a limit could be set on the value of payable orders and other transactions which can be processed by each member of staff.

For example, financial applications may be configured to allow finance administration staff to commit expenditure of up to £10,000, whilst more senior staff would be able to commit expenditure of between £10,000 and £100,000.

Although limit checks review the correctness of data, they can be used to provide assurance that the figures are reasonable. The limits should be set so that all good data is accepted and data which is obviously wrong is rejected. It is up the client to decide what limit to apply bearing in mind the patterns of expenditure.

Limit checks can be linked to individual users. For example an ordinary purchasing clerk can enter and process purchase orders up to a certain value, (say £100,000). however. Purchase orders in excess of this amount need to be entered by someone with a higher authorisation limit, e.g. the finance department's manager or supervisor.

Check digits

Check digits are used to check transposition, transcription and random errors. The control involves the calculation, using a pre-defined formula, of a check digit based on the number to be entered. The check digit is then added to the end of the input number.

For example, if a number 12345 was to be entered and the check digit was based on a modulus of 11 and a weighting of 7, 5, 1, the check digit would be calculated as follows:

1 * 7 = 7

2 * 5 = 10

3 * 1 = 3

4 * 7 = 28

5 * 5 = 15

Total = 63

63 divided by the modulus 11 = 5 with 8 remaining.

Therefore the check digit is 8 and the number entered by the users would be 123458.

Some systems use the power of 2 as a weighting, therefore instead of 7,5,3 in the previous example a weighting of 2, 4, 8, 16, 32 would be used instead.

Most check digit systems use a modulus of 11.

Data validity checks

Validity checks involve the computer automatically checking data entered by a user to a known set of values of figures. If the input does not match a pre-defined figure or value the input is rejected.

For example, if a finance user wanted to enter a transaction against a specific account code, the application would check the account code being entered by the user against the pre-defined chart of accounts. If the account code is not within the chart of accounts the transaction is rejected.

Validity checks on account codes reduces the risk of mis-postings or transactions ending up in limbo (i.e. not summarised in the trial balance or accounts).

The auditor should be aware that with some applications, when the system is unable to validate data it may instead add the new data to the table. For example, if a system did not recognise an account code for a transaction the system would let the user know by displaying a message "account code unidentified" and then ask if the user wanted to add the account code to the account code table. This can cause problems where these new account codes are not picked up by reporting systems. In this example the new account codes may be missing from the routine which prepares the trial balance and summarised accounts.

Validity checks on standing data such as a list of approved suppliers reduces the risk of fraud (provided that the permissions required to update the standing data is restricted).

Compatibility checks

Compatibility checks are used when there is a definable interrelationship between two sets or fields of data. The relationship between the two fields should be defined and recorded (usually in a table). When sets of data are entered the they are compared using the relationship in the table. For example, if a user enters a date of birth, followed by the age of an employee into a personnel system using the values of 1 April 1968 followed by an age of 78, the application would reject the data (the correct age should be approx. 28).

16.3.4 Duplicate checks

The increase in the number of transactions that need to be processed has played a large part in the computerisation of accounting systems. Unfortunately, the increased volume of transactions has resulted in finance staff being less likely to remember transactions they have previously processed. This problem is added to by the fact that one computer input document may look very similar to another.

This increases the risk that duplicate transactions will occur and remain undetected.

To address this risk, some applications may be able to detect duplicate transactions, e.g. by comparing new transactions with transactions previously posted to the same account. Other systems flag transactions after they have been actioned. For example, invoices in a supplier's account would be flagged once payments have been made.

Other systems may only accept a certain number of transactions per account, unit or individual. For example a time recording system would only allow one timesheet to be entered for each employee.

16.3.5 Matching

This control checks and compares one transaction record against data contained in another related transaction. Where data is found to differ an exception report is produced. For example, the data entered when goods are received are automatically compared to the supplier's invoice and the purchase order data on the system. Where a mismatch is found the computer produces an exception report. The client should then take steps to identify the cause of the discrepancy.

16.3.6 Dealing with rejected input

It is important that, where data is automatically checked and validated at data entry, there are procedures for dealing with transactions which fail to meet the input requirements, i.e. the auditor should determine what happens to rejected transactions.

There are alternative methods of dealing with input transactions which fail validity tests.

Rejected by system - Where transactions are rejected outright the client should have procedures in place to establish control over these rejections and ensure that all data rejected will be subsequently corrected, re-input to and accepted by the system. The system rules will determine whether individual transactions or complete batches should be rejected.

Held in suspense - in this case it is critical that users recognise the placing of items in suspense as a prompt for action. It is essential that all items held in suspense are corrected and ultimately successfully processed. In adopting this approach, we overcome the possibility of rejected items being lost but delay the recognition of the need to take action to correct the input error.

Where items are held in suspense the auditor should review the procedures for identifying, correcting and clearing these transactions.

16.3.7 Exercise on input controls

This exercise relates to GOSTF's sister organisation The Building Supplies Trading Fund (BSTF).

Scenario

The Building Supplies Trading Fund employs 4,131 staff as follows:

Category	Description	Number
1	Manufacturing workers	3500
2	Manufacturing supervisors	177
3	Factory managers	10
4	Sales managers	10
5	Salesmen	188
6	Maintenance engineers	80
7	Maintenance supervisors	8
8	Maintenance manager	2
9	Storemen	30
10	Stores manager	6
11	Other manual employees	20
12	Admin. staff	100

Employees in categories 1,2,6 and 7 are paid weekly in arrears, an their gross pay is dependent upon an aggregate of four hourly rates, i.e:

1. The basic rate, applicable to all hours worked;
2. The full rate, which is applicable to all hours over 20 per week;
3. The overtime rate, applicable to all hours worked in excess of 39 per week.;
4. The efficiency rate, payable on all working hours and based upon the efficiency of each work section in the previous ten weeks. The rate is reviewed every four weeks.

Employees in categories 3, 4, 8 and 12 receive an annual salary paid monthly.

Categories 3, 4 and 8 receive an additional bonus as a percentage addition, which is based upon production efficiency for each works section or sales section over the previous quarter, and applying quarterly in arrears.

Employees in category 5 are paid a monthly basic salary plus a commission, based upon an employees seniority and sales. The commission rates are reviewed every 6 months.

Employees in categories 9, 10 and 11 are paid a basic hourly rate, paid weekly in arrears.

Staff in categories 1, 2, 6, 7, 9 and 10 complete weekly clock card which show time on and time off. At the end of each week clerical staff complete the cards by entering the hours worked each day and the total for the week.

Staff in category 11 complete weekly time sheets which record time on and off and other hours claimed. These are checked by clerical staff and certified by the supervisor.

Staff in categories 3, 4, 5, 8, and 12 keep register of attendance, absence and other pay items. For category 5 staff the register is completed in arrears as daily sales reports are received from salesmen. Four weeks before the end of each month each section office completes a return (Variance return) which shows, for each member of staff, departures from standard pay. Any corrections for the last four days appear in the next moths return.

Productivity data is transferred by disk each week in arrears from information generated by the Works department. The data is logged into the pay system and used to calculate productivity rates and bonuses.

Sales data (for the quarterly efficiency review) is produced before the end of each quarter by the Sales team. These are passed to the pay section who enter them to calculate the productivity of the sales section and the bonus payments to sales managers. Twice a year the pay section produces a printout for each salesman, showing seniority , sales analysis, commission record. A space is left for new commission rates to be entered as authorised. The new rates on this printout are manually approved and entered into the payroll system.

Weekly paid employees receive their pay by cash or cheque.

Monthly paid employees are paid by cheque or direct transfer to their bank accounts via the Bankers Automated Clearing System (BACS). BSTF sends a tape to the bank each month.

Data input is via a keyboard terminal in the personnel section.

You are required to:

1. Identify the various types of input relating to pay and the data to be entered (exclude pay rate changes and deductions e.g. taxation);

2. Specify how BSFT might batch input data (from 1 above) for processing and the data that would be used as batch totals;

3. Specify how the data could be checked at the data preparation stage, immediately prior to keying in;

4. Provide examples of the type of data validation that could be applied on data entry.

16.4 Processing control techniques

Processing controls should ensure that:

- the data has been property processed;
- all the data has been processed;
- the data has only been processed once; and
- processes have been applied to valid data.

Processing procedures and controls are likely to be more efficient where they are automated.

Processing controls can be said to operate at two basic levels:

- at a transaction level : controls are applied to individual transactions as they are processed; and

- at a total level : total controls are applied to groups or records and are usually used to ensure the completeness of processing.

16.4.1 Run to run controls

Where it is possible to identify a total derived from a file to be processed which will remain intact through and after the processing of the data, the agreement of this 'before' total to the file of processed data, the 'after total', is a very effective means of controlling the completeness of information processing.

Where a number of processes will be performed successively it may be possible to extend this principle to agree a total derived from data prior to the first process through to the file total following the final process performed. This is only possible where a unit of control can be identified which will survive through the course of all processes but even where this is not possible a run control can sometimes be achieved by the use of a pivot total or checkpoint total.

Pivot or checkpoint totals involve the exercise of control with reference to one total up to a point in the processing where it is possible to relate two totals and exercise control from that point forward by means of the second total. A good example of the use of a pivot total is a time recording/payroll system which establishes a control total from hours worked up to the point where this can be equated with a value for gross pay and then adopts this as the control total from that point onwards.

Where run to run controls change from one process to another it may be an indication that data has been lost or added to whilst being processed. When out of balance run to run totals are discovered they should be reported to the IT department for investigation.

Control totals can also be used to detect processing errors in non-numerical data, for example if the name of a supplier or cheque payee is corrupted during processing. This can be

achieved by using hash totals. Hash totals are calculated by applying an algorithm to a non numerical data field and producing a numerical total. For example, a hash total can be applied to an employee's national insurance or tax code.

Hash total example : each alpha and numeric character is assigned a value. The value of each field, e.g. the name of an employee is calculated using the assigned values, e.g. the character A=1, B=2, C=3 etc. The field value is known as the hash value. The hash values for all the records in the processed file are added to produce a hash total. Since the names of the employees should remain the same throughout, the hash total should not change.

For example, the hash total for a suppliers name ABC rentals Inc. could be 122937. If whilst processing this ended up a ABD rentals Inc. the new hash total could be 122939 and the system would produce an exception report.

Hash totals can also be used on datafiles to detect if any unauthorised amendments have been made. E.g. an application with a self integrity checking control could use a hash total technique on its underlying database. The hash total could be calculated whenever a processing cycle is complete or before the computer is turned off. When the computer resumes processing it could recalculate the hash total and compare it to the previous total. If they are different it could be that the underlying database has been altered via a back-door route.

16.4.2 Independent control accounts

Where a control account receives postings from a source which is independent of the data to be processed, the control account can be used to predict the results. Where the processed results are significantly different the discrepancies can be investigated.

Where there are sufficient alternative controls over the input of data to the system, this control account can be posted from accepted input totals. However, if the client intends to adopt this approach as a control over the completeness of input to the system as well as over processing performed, it is necessary to post the control account from a source which is external to the system.

Unlike the use of run to run control totals, the use of independent control accounts is effective in flagging errors caused by factors other than the transaction data being incorrectly processed. For example the independent data can reveal errors which arise from the use of an incorrect ledger file in the course of a processing cycle. E.g. last months file instead of this months.

16.4.3 Data file control records

The use of data file control records is intended to ensure that all data records on file have been correctly updated to reflect the processing performed. A control record is maintained as part of a data file and contains a total of the number and value of records on the file, e.g. 100 records with a sum of £120.

Each time a process is applied to the file, the accumulated totals of the file updated are applied to the control record, e.g. 12 records added with a value of £15. At the end of each

process, an accumulated total of file records is compared with the contents of the control record, any variance highlighting an error during processing.

16.4.4 Transaction validation controls

Where data is transferred from one application to another, the receiving application can carry out data input checks previously described in this chapter, e.g. range, reasonableness, data validation checks etc. In addition whilst transaction data is being processed, validation checks can be performed to ensure that the output is reasonable and accurate.

16.4.5 File reconciliation controls

File reconciliation controls are carried out on two of more files which contain similar or related information. The files are compared and any differences reconciled. For example one file may contain bank reconciliation information and the other may contain a list of receipts and payments. The two files can be compared and differences explained.

16.4.6 Discrepancy handling procedures

The auditor should determine how the application and users deal with discrepancies, including whether transactions are rejected during processing and what procedures does the client have for rectifying the error and resubmitting the data.

16.5 Output controls

Output controls should ensure that:

- an output is produced when an output is expected;
- the output is complete;
- the output is accurate and is as processed;
- the output is reasonable in terms of quantity and format;
- output is produced timeously; and
- output is distributed to the right destination in a secure manner.

16.5.1 Expectation of output

Those submitting data for processing or responsible for resource budgets should have a fair idea of what to expect and when they are likely to receive it. An expectation can be created through experience and user training. For example, after a while users will come to expect to receive a budget report at the end of each week or month, so if they don't receive the expected reports they will attempt to find out why.

A more formal approach to ensuring that users receive output after they have submitted data for processing would be to keep a log or schedule of data sent, and output received. The log can be manual or computerised.

16.5.2 Completeness of output

The completeness of output produced from a system can be established by the accumulation of totals derived from information contained in the report. These total would then be printed out at the end of processing. These totals can then be compared with a total predicted by the balance on an independent control account or the contents of a data file control record.

With some reports it is not possible for the total of items included to be agreed or reconciled to input data or totals as outlined above.

The completeness of computer output can be ensured by automated controls such as programming the application to add sequential numbers to output reports, i.e. page numbering. This would allow users to quickly identify missing pages. Similarly the system should print "end of report" on the final page. Alternatively printing 'x' of 'y' can provide the user with assurance that the output is complete.

Where a user requests a report, but no records or data is extracted the application should be programmed to print the words "NIL REPORT".

16.5.3 Protection of application output files

Many financial applications do not immediately produce an output when the user presses the enter key. Instead they process a file or group of transactions and store the output in a temporary file awaiting output to a printer (i.e. spooled output).

Where output is held in a temporary location, the auditor should ensure that there are appropriate logical access controls to stop any unauthorised amendments to the data.

16.5.4 Reasonableness of output

The output produced by the computer system should be reasonable and meet the user expectations.

The initial responsibility for checking the reasonableness of computer output may rest with either the user or the IT department. Where the users has control of the data input, processing and output s(he) will be responsible for checking the reasonableness of output. Where data is sent to a central IT department for keying in and processing the IT staff would be responsible for initial reasonableness checks (e.g. if the system produces a 50 page report when a 5 page report is expected).

Ultimately the systems are designed to process users' data and it is they who have the final responsibility for ensuring that the computer output is reasonable. After all it is their information, their resources and they are the ones who have to make decisions based on the information they receive.

16.5.5 Output is produced timeously

Controls within the IT department should ensure that users' data is processed and that any output is available within a reasonable time.

The speed and timing of output will be influenced by business requirements. Some parts of the client's business may depend upon timely reports and up to date information, e.g. users

who deal with equity markets, whilst others may be able to wait a few days, e.g. quarterly sales reports.

16.5.6 Distribution of output

The distribution system operated by the client should ensure that output is delivered to the right people, in the right place within a reasonable time.

The security requirements of distribution systems will be dependant upon the sensitivity or value of the output. For example, the output from a cheque writing machine would be subject to a higher degree of protection than period end budget reports.

16.6 Use of report writers by system users

Modern financial applications frequently include in-built report writing modules which allow users to specify their own customised reports.

Users can use report writers to specify what data they want from the database. Many report writing modules have a user friendly front end and an underlying database enquiry language such as SQL. Once users' reports have been processed, they can often be downloaded into off the shelf spreadsheet packages such as Excel or Lotus.

There are a number of control problems which arise where users produce their own reports based on their own logic and their own timescale. Where the client make use of user defined report for financial reporting purposes, the auditor should review the use of such facilities and identify the risks which are specific to these circumstances and which must be considered in addition to the points raised previously in this chapter.

At the system design stage, the client may not formally decide or specify which principal reports are to be predefined. Where this is the case the may be little consideration given to how users will establish that the reports produced by the system are appropriate or accurate.

User defined reports are more likely to incorporate errors, particularly as they are not subject to the same rigorous testing as reports specified up front in the early stages of a system's development.

Potential sources of errors include:

- the logic under which items on the report have been selected may be incorrect;
- the information may not be complete or up to date at the time of extraction e.g. there may be some transactions still to be processed;
- all the relevant information may not have been accessed by the program due to software failure; and
- breaches of security (e.g. sensitive or personal data may be extracted and disclosed).

At the system design stage a small number of reports should be defined to demonstrate to the user, the accuracy of the system information. Specifically these reports should give assurance that:

- all authorised input has been properly processed;
- only authorised input has been processed;
- transactions from other systems have been properly and promptly processed;
- transactions have been processed using the correct file versions;
- transactions generated by the system for input to other systems are correct and timely; and
- the information on the system continues to be correct and has not been corrupted in any way.

The extraction logic, e.g. SQL which has been used to produce a report should be printed on the face of the report. This creates an audit trail and allows both users and the auditor to carry out subsequent checks and reviews as required.

Furthermore, it may be prudent to restrict the selection criteria available to users to certain straightforward functions. This would reduce the risk of common logic errors.

Users' access could be restricted to standard selection criteria and report layouts which only require minor amendments. These standard reporting criteria should satisfy the majority of ad hoc reports which the users are likely to require.

Many popular accounting systems include fairly sophisticated report writing facilities. Access to these and control over the use of any reports generated should be carefully reviewed, especially since some report writing systems have the ability to write back to a data-file.

Some indication should be printed on the reports to show how up to date the information is. This would be application dependent and would consist of at least the time and date that the information was extracted and preferably the last time that the relevant file had been updated from each of its feeder systems.

Where the file which the user is reporting from is static e.g. from a previous month end this would be reasonably straightforward. Where the file which the user is reporting from is dynamic e.g. in mid-month data then some indication of status may be crucial.

Finally, there should be some indication that the program has accessed all of the relevant records on the file. Again this would need to be considered for each individual application. For example where reporting is from a "static" file, a total of all records read could be printed and agreed to the control reports suggested at above. Alternatively in a "dynamic" file there could be some message confirming that the total of records read agree to a control record held on the file. This control record would in turn need to be reconciled to external totals on a periodic basis.

Paramount in all the above is an acceptance by users of the need for such controls and a clear definition of the circumstances under which such controls need to be exercised and by whom.

16.7 Real time systems

Real time systems are becoming increasingly common as manager demand the immediate availability of up to date information. The increased performance of computer systems has provided software developers with hardware platforms which have the processing power to carry out real time processing.

16.7.1 Loss of conventional control mechanisms

Where a system supports real time processing, it will not be possible for the client to implement many of the batch orientated system control procedures upon which management and auditors have traditionally relied.

The control consequences of real time processing can be summarised as follows:

- direct terminal input can result in the users' failure to prepare or retain source documents with a consequent loss of the traditional paper based audit trail;
- real time transaction processing eliminates the need to batch input and so completeness of input cannot be ensured through reconciliation of input and output batch totals;
- interactive, on-line editing removes the need for input error reporting. Hence it is not always possible to obtain evidence to establish whether validation routines have been working properly;
- control totals are not generated by any of the functions of the system and so control over run-to-run processing cannot be established by this means;
- information is entered and retrieved from the system as required and there is often a lack of reporting of complete data files which are ready for processing. For example entering employee payroll amendments before an month end payroll run, the personnel staff may not know when all the amendments have been made; and
- there is no formal procedure for the update of master file information and changes are not reported on a regular basis.

16.7.2 Preventive controls in real time systems

In many cases there are a number of preventive controls which application designers can build into real-time systems which are designed to reduce to a minimum the possibility of errors. Common control techniques include:

- logical access controls such as password protection of the application and key functions can be employed to prevent unauthorised access to modules, sub-modules or input screens. (logical access controls have already been covered in chapter 17);
- real time input controls can allow the application to validate input data at the time of entry, together with the immediate correction of any information which has been entered incorrectly and rejected by the system;
- log files can be used to record activity on the system. Where logs files record security incidents, such as failed access attempts, they act as a deterrent against the temptation to experiment. If users know that the system will record their unsuccessful access attempts they are less likely to try; and

- integrity checking : this control can be used to identify inconsistencies at the earliest possible point in time. For example, an integrity checking control may be able to detect if any unauthorised editing has been carried out to the datafiles of database using data amendment or editing tools. This will reduce the risk of changes being made via back-door routes such as the operating system.

16.7.3 Detective controls over real time systems

Due to the inability of conventional control techniques to effectively control information processed in real time applications, the available alternatives must be considered and the most appropriate adopted for each. These alternatives include:

- one for one checking - the acceptance of each transaction onto the system is confirmed individually by the initiator. This is only practical where a complete record of all transactions entered is available at a point subsequent to the entry of the data. This control technique is most suitable for applications which have a relatively low volume of transactions to process;

- retrospective batching - identifiable batches of information are constructed retrospectively from transactions entered into the system and agreed with the accepted information in a manner similar to the approach adopted for batch processing systems. To allow this method of control to be operated, the system must be capable of collecting together the information and treating them as a batch for reporting purposes;

- exception reporting - reports are produced from the system of all transactions which do not conform to pre-determined criteria. The likely criteria for reporting include: large transactions, items without time parameters, information inconsistencies, reconciliation failures. This control includes the inherent assumption that no action is required on the other transactions;

- suspense account reporting - all transactions which cannot be processed by the system in the normal way are posted to suspense accounts. Any suspense account balance should be reported and regarded as a prompt for action to be taken to resolve the processing problem; and

- external control accounts - information processed by the system is independently posted to a real control account outside the computer system and reconciliation between this account and the computer system total relied upon to ensure completeness and accuracy of processing.

It is frequently the case that several of the techniques listed above are employed concurrently to achieve control over a system. The controls can be used to exercise control over different parts of the system and they should be designed to support one another. In all cases, the control structure most appropriate to an application should be adopted.

16.8 Database systems

Many of the controls difficulties identified in real time systems also apply to database systems. Database systems also have added problems in that the auditor will be required to rely to a greater extent on the general controls within the general computer environment (i.e. the computer installation).

This is because application controls alone are unlikely to be capable of ensuring the completeness and accuracy of processing performed by database systems. Application controls may be effective in controlling what data is entered via the applications data input screens , however they are usually unable to prevent alterations to the underlying databases. The auditor should review the general IT controls to evaluate the controls that reduce the risk of users directly editing the database.

16.8.1 Control problems specific to database systems

Where systems use a database to store transaction details, the client will normally appoint someone to look after database administration duties. This person is called the database administrator.

In order to effectively perform his/ her role, the database administrator is given a great deal of power and will be allowed access to all information on the database. The administrator will have high level access privileges and will be capable of performing many more functions than an ordinary system user.

Relationships between data elements within a database can be very complex and so it is difficult to establish the continuing integrity of the database and consistency of the data relationships. There are utility checking programs available for most databases which can be run periodically to ensure integrity but it may be very difficult to establish the cause and source of any errors which are found.

The completeness of reporting from a database is dependent upon the accuracy of the pointers between data elements rather than the ability of an application program to read successively through a file. For this reason it is necessary to treat all reports from database systems as exception reports whose completeness requires to be proved rather than accepted without question.

If a database is updated in real time, then the status of the data included on back-up copies of the database is likely to be variable, depending on the position of that data in the back-up sequence. If the client has needed to recover the database from a back up source, the auditor should review the procedures adopted to ensure that transactions submitted during the back-up process are included.

16.8.2 Ways of compensating for control weaknesses

As it is very difficult to prove that database functions are actually working properly during the course of processing data, great care must be taken in the specification and development of database functions and comprehensive testing should be carried out prior to system implementation.

Where there have been no changes since implementation, the auditor may be able to place reliance on the testing procedures and test results. Where practical, it is advisable to reprocess test data periodically to ensure that identical results are produced.

Database integrity checking should be regularly performed and all errors fully investigated and corrected by the database administrator. The cause of errors should be established and functions amended if necessary. Where functions are changed an appropriate level of re-testing should be carried out.

Database testing should include the testing of back-up and recovery procedures. The auditor should review any documentation the client has on recovery and back-up procedures. The documentation should cover the various courses of action which may be taken to implement both short and long term database recovery. The testing and back-up plans should be clearly understood by all relevant personnel.

The duties and responsibilities of all client staff involved in the administration and control of the database should be clearly specified and documented. Database documentation should also include descriptions of the functions of all applications requiring access to information on the database.

The auditor should determine if the client's data dictionary is up to date. Some trainees may need reminding of what a data dictionary is. A data dictionary is a description of the database, which holds the names and structures of all data types as well as any constraints on data and which applications use the data.

Database resilience can be achieved by:

- checkpoint, dump, restart controls : where periodic dumps are taken as checkpoints and transactions are recorded between checkpoints. When restarting, the system takes the last dump and reapplies the transactions; and
- roll back and roll forwards :this refers to the ability to undo transactions or reapply them, hence allowing the database administrator to determine the state of the database at any point in time.

16.9 Distributed systems

The use of distributed systems is on the increase. The increased capacity and lower cost of communications systems has allowed previously unconnected systems to link together. Software suppliers have developed new applications which take advantage of processing capabilities at both end of a network, i.e. client server technology.

There are a number of control concerns which are specific to the control over distributed systems. These are in addition to the concerns and techniques covered earlier in this chapter and arise as a result of the technology employed and the physical and logistical spread of data within distributed systems.

16.9.1 Control over data communication

When data is transmitted between inter-connected devices using communication facilities, it is essential that it can be ensure that there is no corruption of the data in the course of transmission and that the files receiving the data are completely updated.

Most communication facilities provide automatic integrity checking mechanisms using a variety of parity and redundancy checking techniques which give a fairly high amount of assurance that the transmitted data is error free.

To ensure that data files on the receiving device are fully updated, reports of data transmitted and received should be independently produced, one at each location, for comparison purposes where this is practical. Where the transmission of a large volume of data is involved, an alternative means of ensuring the completeness of update of the receiving file must be identified.

16.9.2 Control over access to system functions

Where processing power has been distributed to a number of separate locations, it is no longer appropriate to place substantial reliance on the physical access restrictions to a central computer suite.

As an initial precaution, steps should be taken at each distributed location which has access to processing facilities, to restrict access to only authorised personnel.

The client should then consider the processing needs of each location. The system should be configured to restrict the access to the information and facilities actually required. This is likely to involve the preparation of a complex matrix matching requirements with facilities. The matrix should be centrally maintained and regularly updated to provide a record of the authorised users of all facilities available within the system.

Logging of activity on the system should provide sufficient details of updates performed. This should allow the source of amendments to information to be established in the event of an error or a failure to successfully update the central database. Close monitoring of the system is required to allow system administrators to identify and rectify any difficulties within an acceptable timescale.

16.9.3 Control over consistency of data

If copies of data files are maintained at different points on the system the client should ensure that consistency is maintained. This can be achieved by:

- all updates are reflected in all files. In this case there will be complete consistency of data in all files at all times. The control system co-ordinating activity must be capable of ensuring that all updates are properly reflected on each relevant file and of detecting and correcting errors where the update of one or more file copies is not successfully achieved;
- all updates are reflected only on a central file. A central definitive version of the data file is maintained and all update programs will access only this file. Local copies of the file are provided for enquiry purposes only and are overwritten by a copy of the central file at regular intervals. Local files will be out of date at any point in time to

the extent of all updates that have taken place since the most recent copying from the central file.

17 Masterfile and standing data controls

17.1 Introduction

Masterfiles are data files which contain semi- permanent financial or reference data which may be used by several applications to process. The data stored in the masterfile is known as standing data.

Applications call upon the reference data in masterfiles to process their transactions.

For example, a masterfile may contain standing data on the price of goods for sale. When a sale is made the application requires the user to enter the variable transaction data such as the quantity of goods sold. The application then calls upon standing price data in a masterfile and combines the unit price with the quantity to get the total value of the sale.

Standing data may include:

- pay rates for each grade;
- supplier details (reference number, address, telephone number, credit terms);
- customer details (name, address, telephone number, credit limit);
- employee bank account numbers (for automated payroll transfers);
- inflation rates and indices(for current cost accounting);
- overhead rates;
- system administration data, such as password files, or access control permissions; and
- account codes.

17.2 The importance of masterfiles and standing data

Due to their nature, standing data is used to process many transactions. For example the VAT standing data may be used to determine tax liabilities on hundreds or thousands of an organisations transactions.

It is therefore very important that the standing data is right. The auditor is concerned with standing data because one standing data error, combined with the systematic nature of computer systems will result in large errors in the client's accounts.

The client should have recognised the importance of standing data and should have controls in place to ensure that :

- amendments to standing data are authorised;
- users are held accountable for any changes made;
- the standing data is up to date and accurate; and
- the integrity of the masterfiles is maintained.

As standing data errors have a far reaching effect it is normal for the controls over the data to be more stringent than controls over individual transactions.

17.3 Masterfile controls

The type of controls a client may use to protect standing data have already been covered in this module, i.e. physical and logical access controls (identification/ authentication resource protection and logging).

These controls should ensure that only authorised users can gain access to, create, amend or delete standing data.

The controls may be implemented at both the application level and the installation level. The installation controls should ensure that other computer users, e.g. IT operations staff and users of other applications cannot gain access to the data. The application level controls should ensure that only application users who need access to standing data are granted access.

Another control the client may use is segregation of duties, i.e. those responsible for entering transaction data should not also have the ability to make amendments to transaction data. In the fraud examples losses occurred because users had the ability to set up standing data and then initiate transaction which rely on the standing data.

Individual transactions have to be authorised and the same principal applies to changes to masterfile data. Hence the client should have procedures and controls for making amendments to masterfile data. These may include filling out data amendment forms or having one user enter the amendment and another user (supervisor) commit the amendment using automated permissions.

Audit logs are useful as they can help identify individual users who make unauthorised amendments. Ideally the audit log should record what records or fields were amended, when they were amended, from what to what, and who made the amendment.

As standing data is so important the client should ensure that it is regularly backed up, especially after changes have been made.

Client management should ensure that independent checks are carried out on the masterfile data. The client may periodically print out copies of masterfile data and checks a sample of data to ensure that it is up to date and correct.

Where users have to request masterfile changes, it is common for reports on masterfile amendments to be printed out. The printouts are then sent back to the requester for checking.

Standing data frauds

17.4 Example 1

Type of fraud	:	Fictitious employees
Victim	:	Health Authority
Perpetrator	:	Wages clerk
Method	:	The wages clerk made use of her knowledge that the list of employees and the personnel salaries list could not be cross-checked for fictitious employees. She added fictitious employees, including two highly paid doctors and a registrar to the payroll systems standing data file which contained payroll data. The fictitious employees were made to look real by giving them wage rises, overtime payments and extra duty allowances. She even went as far as to create promotion records for her employees. For eight months she extracted the pay cheques produced by the payroll system and put them into bank accounts in three separate branches. She managed to open bank accounts for each of fictitious employee using their made up names and her real address.
Value	:	Over £5,000 (1975 value).
Discovery	:	At the time the fraud was perpetrated the internal auditor responsible for reviewing the payroll systems was off sick and the internal audit department was short staffed. When he returned from hospital the fraud was quickly discovered.
Penalty	:	The perpetrator admitted seven charges of theft, five of false accounting and three charges of forgery. She was jailed for a year.

17.5 Example 2

Type of fraud : Unauthorised use of standing orders.

Victim : Major construction company.

Perpetrator : Senior accountant.

Method : The senior accountant had been employed in a position of trust in the company for several years. He found that the new computerised general ledger system provided a means by which he could easily defraud his employers. He set up a bogus company with a fictitious address on the suppliers validation database He then used his terminal to access the masterfile which contained data on standing orders. He set up a standing order to pay the fictitious company £30,000 per month. As the validation reports were sent to him, he could ignore the data and destroy input documents to remove evidence of the transactions having occurred. He then sat back and waited for the money to appear each month. The fraud went on for 9 months. The culprit bought a big house and the usual luxury items. the rest of the money was deposited in a savings account.

Value : £250,000.

Discovery : The fraud was discovered at the year end company audit. The company recovered most of the money from his savings account.

Penalty : He was dismissed and prosecuted.

17.6 Example 3

Type of fraud : Bogus pensions and annuities.

Victim : Large insurance company.

Perpetrator : Pensions superintendent in collusion with clerk and relatives.

Method : The fraud began in 1970 while the culprit was working in the department responsible for recording new pensions and annuity payments. He created fictitious individuals in the pensioner masterfiles, prepared the documents and authorised the payments, using at least 24 bogus beneficiaries over 15 years.

Payments were made to a building society and bank accounts set up with false names. This allowed him to also defraud the taxman.

The clerk was involved as he took cheques prepared by the computer and ensured that the records were not copied onto microfilm records.

The superintendent admitted to the police that he stole over £400,000 and the clerk admitted to having received over £90,000.

The superintendent arranged for £22,764 to be paid into his sister-in-law's bank account in her maiden name. She was due to legitimately receive £687 in annual payments, but the perpetrator altered the standing data to increase the figure to £6,870.

Amount : £520,000.

Penalty : The superintendent was dismissed in 1985. He was found guilty and given 5 three and a half year concurrent sentences. The clerk admitted conspiracy and was given 2 years.