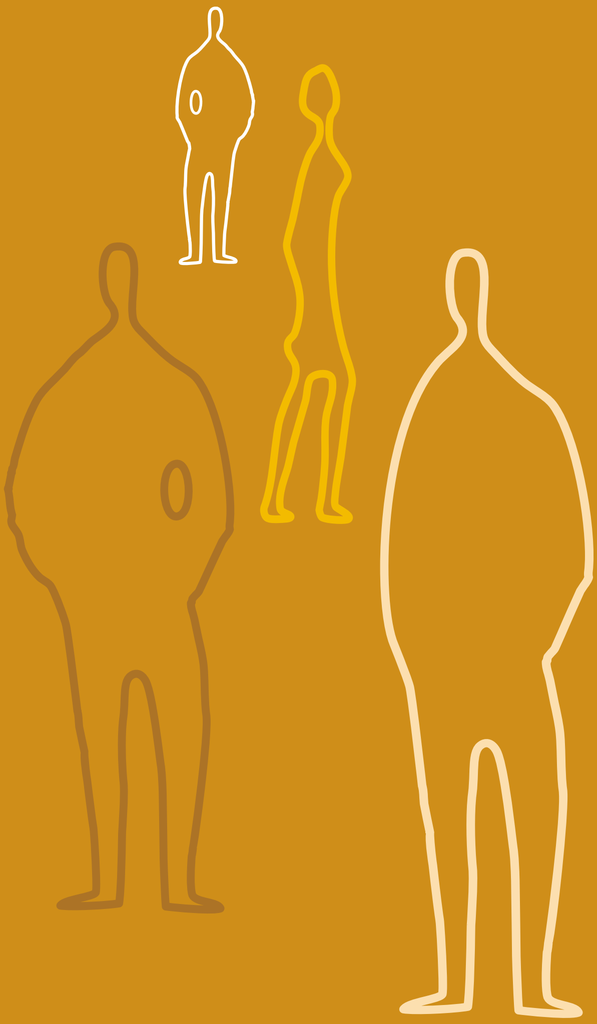
An Introduction to Computer Auditing



Barclay Simpson
Recruitment Consultants

Index

1. Introduction

1.1 Purpose

The aim of these notes is to give potential computer auditors an overview of the main activities of computer audit and the role of the computer auditor. They have been written to assist candidates who are planning to attend an interview for a position in computer audit but have a limited knowledge of the subject. For those from either an audit, business or information technology (IT) background seeking a move into computer audit, these notes will provide useful background reading.

Whilst any organisation that has agreed to interview a candidate who has limited experience of computer auditing will judge them accordingly, there is substantial scope for candidates to improve their chances by demonstrating that they have done some research and are conversant with the basic principles.

Further, as it is increasingly difficult to distinguish between IT and business areas, many organisations now require that all business auditors have an awareness of computer audit. These notes, therefore, should assist business auditors in obtaining a greater appreciation of computer auditing.

Given the diversity of IT, it is not possible within a document of this type to be specific about computer audit in particular sectors or in relation to specific hardware or software. The basic principles of computer audit should be common to all sectors and to most types of hardware and software.

1.2 Definition

One of the most important factors to consider when discussing computer audit is that the term “computer audit” can mean many different things to different people. What may be regarded as computer auditing in one organisation, and very much the realm of the specialist computer auditor, may be undertaken by business auditors in another similar organisation. For example, computer audit may be restricted to auditing systems software in one organisation, whilst areas such as auditing systems under development may be the responsibility of the business auditor. Similarly, in some organisations, it is not uncommon for the role of computer audit to be extended to include the review of clerical procedures and the production of compliance based audit work programmes for field auditors, thereby providing a wider systems audit service.

There are no hard and fast rules as to what constitutes computer audit. Often, similar sized organisations operating in the same sector may have different approaches to computer audit. Even where there appears to be commonality in the scope of audit areas, there can be significant variations in the depth of auditing undertaken. An audit of an operating system in one organisation may require between 5 and 10 man-days, whilst in another, the same operating system may be subject to a more detailed examination lasting several months.

1.3 Origins of Computer Audit

The absence of a common definition of computer audit may, in part, be due to the relative newness of computer audit. The history of traditional auditing or inspection can be traced back many hundreds of years. In contrast, computer audit is a relatively recent development. It was not until the late 1970’s that the majority of major organisations in the UK established a computer audit capability for the first time.

The use of IT in business is also a relatively recent development. The father of modern day computing is generally regarded as being Charles Babbage, who produced his Difference Calculator in 1833. It was not until the outbreak of the Second World War and the widespread development of valve technology, that the 1st Generation computers were used. Even then, it was many years later that they became commonplace in business.

1.4 Change

A key feature of many organisations today is change. Although not necessarily the driver of change, IT is invariably an intrinsic component and much of the change would not be possible without IT. IT has had a major impact on social, economic and political factors throughout the world. Not only has it led to the creation of new professions but it has also revolutionised others, such as office work, or, when combined with robotics, manufacturing industries.

Computer audit operates in a climate of constant and rapid change. Computer auditors are continually faced with the prospect of faster, smaller and cheaper IT systems. An analogy that is frequently used to describe the rapid development of IT, is if aviation had developed at the same rate, man would have landed on the moon in 1922. IT is a dynamic area which in turn, requires a dynamic and flexible control structure.

The rapid development of IT is perhaps best indicated by the relative absence of specific IT legislation, which, in England and Wales, is largely based upon precedent established over many years. The only specific IT legislation in the UK at present is the Data Protection Act 1984 and the Computer Misuse Act 1990, both of which have been subject to considerable interpretation by the Courts. Both pieces of legislation are security and control related.

1.5 Nature of Computer Audit

Although an IT system may achieve the same end result as a manual system, the way in which it does so, and hence the level of security and control required, can differ considerably. There are a number of significant risks associated with the processing of IT systems. It is important, therefore, that high standards of security and control are maintained to minimise the potential impact on the organisation.

Computer fraud and abuse can have a detrimental effect on an organisation. Periodic surveys undertaken by organisations such as the NCC (National Computing Centre) and the Audit Commission indicate the following common instances of computer fraud and abuse:

- unauthorised disclosure of confidential information
- unavailability of key IT systems
- unauthorised modification/destruction of software
- unauthorised modification/destruction of data
- theft of IT hardware and software
- use of IT facilities for personal business

When considering computer audit, it should be noted that the basic control objectives and principles do not change. The manner in which those objectives are achieved, however, does change fundamentally. Specifically, there is a need for greater preventative controls rather than a reliance on the more detective and corrective control mechanisms which would usually be found in manual systems. The development of on-line real time systems, where the immediacy of processing can result in millions of pounds being transferred away in a funds transfer system, requires a robust level of security.

1.6 Computer Auditors

It was not until the late 1970's that most organisations in the UK established a computer audit capability. This primarily arose out of the need to provide business auditors with independent data from the IT system. This in turn progressed to a wider review of the IT applications and infrastructure to provide an assurance that the organisation's assets were protected and that suitable security and control mechanisms were in place. The high level of technical knowledge required resulted in the birth of the computer auditor.

It is important when considering computer audit to note that it is an integral part of the overall audit activity. It is usually separated to enable specialised security and control issues to be dealt with more effectively and to make better use of specialist staff. Computer auditing, therefore, is a means to an end rather than an end in itself. There is always a temptation when dealing with IT to become engrossed in the technical complexities of an operating system or application and to ignore the business realities of the organisation. Risk based computer auditing, integrated as appropriate with business audit, is essential if computer audit is to add value to the organisation and to deliver the effective service demanded of it by senior management.

Over the years, the role of the computer auditor has changed to being more consultative and value adding. Clearly, where a new system is being developed, it is more cost effective for audit comments to be provided prior to a system being implemented, when improved security and control features can be included more easily and cheaply. Similarly, although computer auditors regularly undertake audits of say logical access controls, there is considerable scope for computer auditors to be involved in the design of those components.

There is an issue of independence if the computer auditor becomes involved in the design process as this may be compromised if the same individual subsequently audits that system. It is generally recognised, however, that the costs of not getting involved are so great that this is not an option. It is unlikely, for example, that senior management will be happy to receive an audit report just after a new IT system has gone live which details significant security and control exposures.

The role of the computer auditor continues to mature and develop. This is essential if computer audit is to provide a value added service to the business in the face of increasingly sophisticated technology. A key challenge for computer auditors is to keep up to date with the constant and rapid developments in IT. Continuous training and development is essential. Successful computer auditing is based upon a foundation of technical excellence. Without this, computer auditors are limited in their ability to audit effectively and to provide a valuable service to the organisation.

It should also be noted that the role of the computer auditor can, in some areas, overlap with that of the computer security function and this can cause confusion. It is essential to clearly define respective responsibilities so that unnecessary duplication is avoided. Essentially, the role of the computer security section is to assist users in developing security solutions and to administer that security on a day to day basis. The role of the computer auditor is to provide senior management with an independent and objective assurance as to the level of security applied within the IT environment. As an integral part of the audit process, computer auditors will also provide advice and it is in this area that duplication and overlap may arise.

1.7 Scope

The following sections of these notes describe the main areas of computer audit activity:

- systems under development
- live applications
- IT infrastructure
- audit automation

The extent to which these areas are reviewed and the depth to which they are examined will vary. Key to the performance of audit work is a comprehensive risk based evaluation which should determine the amount of audit resource required and should also assist in determining an assessment of a satisfactory level of security and control.

A brief outline of the involvement of the computer auditor has been provided for each area. The purpose of this outline is to give an indication of the audit considerations rather than to provide an exhaustive list. Readers are advised to refer to appropriate text books where additional information is required, specifically, “Computer Auditing” by Ian J Douglas and the “CIPFA Computer Auditing Guidelines” by CIPFA.

Acknowledgement

Barclay Simpson would like to acknowledge the assistance of Graham Burggy QiCA MIIA ACIB, in the completion of these notes. Graham Burggy is an experienced Computer Audit Manager who has worked in computer audit for three major financial services organisations.

2. Systems Under Development

2.1 Background

“There is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage than the creation of a new system” Machievelli.

The development of a new computer system represents an area of potentially significant risk to an organisation. New computer systems are developed to meet a variety of business needs, whether they be to meet new legal requirements, to maintain or enhance profitability, to improve efficiency or to reduce costs. The failure of a new system could have a major impact on an organisation’s future viability and well being.

A review of an organisation’s financial statements will usually indicate that, with minor exceptions, the development of IT systems is also one of the organisation’s major areas of investment.

The potential sources of a new IT application are many and varied. A number of factors, such as cost, time constraints and availability of a skilled resource, will determine which source is the most appropriate for a particular organisation. Options include:

- a bespoke development by an in-house IT team
- a package solution from a software house
- a bespoke development by a software house
- joint bespoke development (partnership) by a software house and the in-house IT team
- end-user development

Computer audit activity within systems under development is focused on two main areas:

- the manner in which a new IT application is developed
- the adequacy of security and control within an IT application

2.2 Development of New IT Applications

It is important to ensure that new IT applications are developed in a controlled manner so that they perform only those functions that the user requires and that adequate security and control is included. The manner in which a new IT system is developed is generally considered under two main headings:

- project management
- the systems development life cycle

2.2.1 Project Management

Project Management is concerned with delivering a solution on time, within budget and to the appropriate level of quality. Project management as an activity is not confined to IT and many of the basic principles have been developed in other industries, notably the construction industry.

The basic principles of good project management are:

- clearly defined management responsibility
- clear objectives and scope
- effective planning and control
- clear lines of accountability

There are a variety of project management methodologies in existence, such as PRINCE (Project in Controlled Environment), which in turn may be supported by an ever increasing range of project management tools, such as Project Manager Workbench (PMW) and MS-Project. The precise requirements of project management methodologies vary and frequently methodologies may be customised to meet the specific needs of an organisation.

In spite of the widespread availability of such methodologies and tools, research has shown that the majority of IT projects are not implemented on time, within budget or to the appropriate level of quality.

Typical components in a project management methodology include:

Organisation
This is to ensure that senior management are committed to the project and to enable issues to be resolved promptly. A standard framework for the direction and management of a project should be established, which generally involves committees such as a Steering Committee and the appointment of specific personnel such as a Project Manager or Project Sponsor.

Planning
This is to ensure that work activities are addressed at an appropriate level of detail, that resource requirements are identified and that risks are properly evaluated. Comprehensive planning is the key to successful project management and forms the basis of subsequent project control. Typically, a project will be broken down into a number of sub-projects, each with a number of specific stages.

Control

This is to ensure that potential problems can be identified and that the ongoing viability of the project can be continuously monitored.

Project control generally consists of financial controls such as budgets and time controls such as milestones, which enable the status of a project to be measured. Frequently, a regime of more subjective controls will also be established, such as internal and quality assurance reviews, supported where necessary by external reviews undertaken by specialist consultancy organisations.

Computer Audit Involvement in Project Management

The computer auditor should be involved in the audit of project management. The purpose of this involvement is to provide an objective view to project management and an independent appraisal to accountable senior management, that an adequate system of project management is in place.

Key areas of audit interest are to assess whether:

- an effective project team has been set up to ensure that responsibilities are clearly defined, that senior management are involved and that issues can be raised
- comprehensive and sufficiently detailed plans have been prepared together with an assessment of the extent to which they are achievable and whether they cover all areas
- effective mechanisms have been established to continuously monitor project progress in order to obtain an assurance that senior management is provided with timely information so that variances from the plans can be investigated and the appropriate action taken

2.2.2 Systems Development Life Cycle

The systems development life cycle is concerned with the formal development of an IT application and aims to ensure that a new IT solution is:

- developed in a controlled manner
- adequately documented
- maintainable in the future
- developed efficiently and securely
- meets the user's requirements

IT applications have traditionally been developed in a mainframe computer environment, in a low level programming language such as Assembler, or a high level programming language such as COBOL, by specialised programmers working to a design produced by systems analysts. Package solutions are also used extensively for common applications such as payroll. As with project management, a variety of methodologies have been developed to assist in this process, the most widely known of which is probably SSADM (Structured Systems Analysis and Design Methodology).

The precise definition of stages in a systems development life cycle will vary according to the development process and methodology being used. In many ways the stages of a life cycle are consistent with the basic principles of TQM (Total Quality Management). Typical stages are:

Project Initiation/Feasibility Study

The purpose of this phase is to progress an initial idea to a stage where a project can be formally defined. Once defined, the feasibility of this proposal and the cost benefit can be determined.

Analysis and User Requirements

The aims of this phase are to confirm the project objectives and scope, to identify and classify the required data and to identify and prioritise business requirements.

Design

The aim of this phase is to complete a logical and detailed technical design of the system which meets the user's requirements.

Build

This involves programming and testing the system. Testing will consist of a number of components, such as unit testing, link testing, systems testing and user acceptance testing.

Implementation

The aims of this stage are to plan and co-ordinate all the activities needed to ensure that the new (or amended) system can be successfully moved into production in a manner which will maximise the delivery of benefits while keeping disruption to a minimum.

Post Implementation Review

The aim of this stage is to review the development to determine any lessons for the future. In practice, this stage is all too frequently ignored.

Increasingly, IT applications are being developed by alternative processes. IT applications, for example, are being developed by end users, whether relatively simple spreadsheets which generate key MIS for strategic decision making or more complex developments in languages such as MS-Access and FoxPro. Even within the more formal and structured IT development areas there is a move towards modern methods of developing IT applications. These include:

- **CASE** (Computer Aided Software Engineering) - this is a working environment consisting of programs and other developmental tools that help managers, systems analysts, programmers and users to automate the design and implementation of programs and procedures. Common CASE tools include IEF, from Texas Instruments, and Foundation, from Andersen Consulting
- **Object Orientation** - a program is viewed as a collection of discrete objects that are self contained collections of data structures and routines that interact with other objects. C++ is an object orientated version of the C programming language
- **Prototyping** - here systems are developed on-screen interactively with the user, typically in a fourth generation language (4GL). Several iterations may be produced until an acceptable product is achieved. From this, a full production system can be developed
- **Rapid Application Development** (RAD) - unlike prototyping which is a development technique to create a throwaway version of a product, RAD is an end to end development life cycle. It is based upon the premise that 80% of the solution can be achieved in 20% of the time it would take to develop 100% of the solution. The most widely known RAD methodology is DSDM (Dynamic Systems Development Method)

A key impact of these newer approaches is that traditional development documentation may not be available. A more interactive and ongoing involvement may be necessary although this in turn may create issues of resourcing and scheduling.

Audit Involvement in the Systems Development Life Cycle

Early involvement in the audit of systems under development is essential. The purpose of this involvement is to provide an assurance to project management, user management and accountable senior management of the organisation that the application has been developed in a secure and controlled manner. Some types of development may cause greater concern than others, such as end-user developments where the users are not skilled in the disciplines of developing IT systems.

The primary area of audit focus should be the design phase where an assurance and advice on the adequacy of proposed controls can be provided. A strong presence in the testing phase is also recommended to ensure that the proposed controls are robust and workable.

The computer auditor should seek an assurance that:

- user requirements have been fully understood and confirmed
- the IT system, and any associated manual processes, meet those requirements
- the development approach and methodology are appropriate for that development and provide for a thorough consideration of risks and the inclusion of controls
- adequate documentation is available which explains the workings of the system

The computer auditor may also undertake limited compliance testing to ensure that deliverables are produced in accordance with the approved methodology.

2.3 IT Application Controls

Within an IT application it is important to ensure that satisfactory levels of security and control are implemented to meet identified risks. Application controls generally fall under two main headings:

- application specific controls
- general IT infrastructure controls

2.3.1 Application Specific Controls

This is concerned with controls within the IT application and consists of the following:

Input Control

Input controls will be necessary to ensure that all data entered is authorised, complete, accurate and entered only once. Typically, a combination of manual and automated controls will be required to achieve this. These include validation checks, range checks and segregation. The system should also provide a suitable mechanism that records sensitive or critical activities by individual users and enables the production of evidence of processing.

Processing Controls

Processing controls will be necessary to ensure that transactions are processed completely, accurately and in a timely fashion. A variety of controls will be used to achieve this, for example, reconciling input control totals with subsequent output, validating the integrity and reasonableness of automatically generated transactions and generating calculations automatically from the appropriate authorised standing data.

Output Controls

Output controls will be necessary to ensure the completeness, accuracy and availability of application output, whether it be in a paper form, or as electronic data. On printed output, controls such as sequence numbers and page numbers will be used to ensure completeness.

Procedures

Procedures should be prepared which contain adequate management and supervisory controls and checks. In some instances, separate user guides may be prepared for the application, although usually they will be incorporated in a departmental procedures manual.

Computer Audit Involvement in Application Specific Controls

Early involvement in the development of a new IT application is essential if the computer auditor is to add value to the process and to safeguard the organisation's interests. It is obviously easier and cheaper to incorporate improved security and control features at the design stage of a new system rather than when it has gone live. Research suggests that it only costs 50p to implement a recommendation at the design phase, but £1500 when it has gone live. In practice, the actual cost can be far higher as the system may not get the necessary priority and resource, and even if it does, the organisation runs the risk of the exposure until the weakness can be corrected.

As the application is in the process of being developed the computer auditor will have to rely on a review of available documentation and discussions with relevant IT and business personnel to obtain an assurance as to the adequacy of security and control. Whilst it is not possible during the development phase to conduct detailed audit testing, formal test plans should be reviewed to ensure that controls are being adequately addressed and consideration could even be given to setting up specific security and control test plans.

Key areas of interest for the computer auditor include:

Input

- are input documents authorised by an appropriate person(s)
- is adequate segregation in place
- does input validation include the following checks:
  - data within valid limits
  - data one of valid codes
  - data compared to existing items on file
  - check digits
  - balancing - e.g. agrees to batch total, journal totals to zero

Processing Controls

- are changes to the calculation/formulae properly controlled, tested and authorised
- are key calculations checked

Output Controls

- is printed output held and distributed securely
- are reasonable checks of output performed
- are logical controls over access to on-line output reports adequate
- is there a schedule of when output is due, which should be linked to an operations schedule to ensure that the necessary programs are run on time

Procedures

- have procedures manuals been prepared which adequately define controls and checks
- have the procedures been tested before the system goes live

2.3.2 General IT Infrastructure Controls

When considering application controls, general IT infrastructure controls should also be evaluated. The rationale behind this is that there is limited value in providing an evaluation on the adequacy of security and control within the application if no assurance can be provided about the IT environment on which it runs.

The basic areas to be considered under general IT infrastructure controls are detailed in Section 4 of these notes. In this instance, they are considered at a lower, application specific level of detail. The extent to which general IT infrastructure controls need to be considered will obviously vary from application to application. If an application is to run on an existing mainframe, then a reliance can be placed upon existing mainframe infrastructure controls. It will only be necessary to consider the areas specific to that application, e.g. which users are to be allowed access, what type of access will be allowed or what additions need to be made to the existing mainframe contingency plan. If, however, the application is to run on a new LAN for example, then additional areas will need to be considered, e.g. should a logical access control package be installed, who will be responsible for its administration and will a new contingency plan be necessary?

The general IT infrastructure controls to be considered include:

- physical security
- contingency planning
- logical access control
- program change control
- operating system
- telecommunications
- storage media
- databases
- cryptography
- computer operations

Computer Audit Involvement in General IT Infrastructure Controls

If the new application will run on an existing mainframe installation, a reliance will be placed upon existing computer audit work to assess the security and control mechanisms in place. The audit effort in this instance will focus on the application specific aspects, e.g. has the application been included in the contingency plan and have appropriate logical access control rules been established. If, however, the application requires a new computer installation, say a LAN, then these areas will need to be considered in more detail.

3. Live Applications

3.1 Background

Many organisations are dependent upon the availability of IT systems to such an extent that it is true to say that for them, no IT means no business. It is important, therefore, that the IT applications within an organisation are subject to a periodic risk based evaluation of security and control. The rationale behind a periodic evaluation is that:

- IT applications are dynamic and changes to the system will be necessary. Although such changes may be subject to audit evaluation, it is usually the case that changes are made over a period of time, usually without audit review, and the application system may differ considerably from that originally implemented. This may impact on the effectiveness of security and control
- the control environment surrounding the application may change. Associated manual processes, for example, may change significantly, as the dramatic de-layering of middle management in many organisations has shown
- live data may indicate the need for additional security and control. As the application is used in a live environment, specific processing conditions or types of data may come to light which the existing security and control structure does not accommodate
- risks may change and increase or decrease, rendering the existing security and controls inappropriate. For example, the number of customers may increase substantially, or data may be used for new purposes such as strategic decision making

In a similar way to the audit of systems under development, effective security and control are achieved by a combination of application specific and general IT infrastructure controls.

3.2 Application Controls

This is concerned with controls within the application - see Section 2 - Systems Under Development for details. For ease of reference, the headings of this Section are summarised here:

Input Controls

- processing controls
- output controls
- procedures

Computer Audit Involvement in Application Specific Controls

The key issue of audit involvement in live applications is to determine who will undertake the review. In many organisations, computer auditors will perform a live review of IT applications, whilst in others, live applications may be viewed as a business area and therefore the responsibility of a business auditor. Increasingly, a joint approach is being adopted by many organisations where the IT application forms part of a wider scope audit of the business area and enables a more integrated and complete review to be undertaken.

The frequency of the periodic review is also important. Risk should be the key factor in determining frequency and hence, importance to the organisation. A variety of risk assessment methodologies are available for this purpose from the simple and subjective to the more formal and structured such as CRAMM (Computerised Risk Analysis and Management Methodology).

The audit work required for a live application review is very similar to that undertaken for a system under development with one main exception. When auditing an application under development, there is little opportunity for detailed audit testing. Audit work will focus on evaluating the adequacy of security and control using discussion and a review of technical documentation. The testing phase of the project may allow some scope for control testing, but this is artificial. With a live application review, there is considerable scope for audit testing, as live data will be available together with other documentary evidence such as error logs.

Effective use of CAATS (See Section 5 - Audit Automation) can also be made in live application reviews. Interrogation software can be used to identify exceptional conditions in data or to produce a sample of records for testing.

3.3 General IT Infrastructure Controls

As with systems under development, when considering application controls, general IT infrastructure controls should also be considered.

These areas include:

- physical security
- contingency planning

- logical access control
- program change control
- operating systems
- telecommunications
- storage media
- databases
- cryptography
- computer operations

Computer Audit Involvement in General IT Infrastructure Controls

The approach to the review of general IT infrastructure controls is very similar to that detailed in Section 2 - Systems Under Development. Again, the main difference is that there is considerably more scope for detailed audit testing in a live review.

4. IT Infrastructure

4.1 Background

IT Infrastructure is a generic term which describes components such as computer hardware, systems software or telecommunications which provide a processing platform for business applications.

IT infrastructure represents an area of potentially significant risk to the organisation as the overall security and control of its business applications is to a large extent dependent upon the level of integrity, availability and confidentiality within the IT infrastructure.

4.2 IT Environment

In considering IT infrastructure, it should be noted that there is no such ideal as a standard computer installation. In some organisations, IT hardware may be located in a purpose built computer centre, where responsibility for its operation and maintenance is in the hands of specialist personnel, such as computer operators, systems programmers and operations analysts. In other organisations, IT hardware may also be located in a purpose built computer installation, but responsibility for its operation and maintenance may be vested in a smaller number of personnel who will perform a wider range of duties. In some organisations, IT hardware may be located in a user environment, where responsibility for such activities as software upgrades and back-ups is simply the part-time responsibility of one or two individuals.

Traditional computer audit text books invariably refer to three distinct types of computer: mainframe, mini and micro. Whilst such terms do exist, in practice it is very difficult to distinguish between them. What is regarded by one organisation as a mainframe computer located in a purpose built computer centre, may be viewed as a mini computer by another and could be located in an office environment. The situation is further complicated by extensive telecommunications networks and the use of client server environments, where several desktop machines are connected to a central server which contains the data and programs. This move towards a distributed computing environment has increased the potential exposure of most organisations as the control environment increasingly becomes dependent on the weakest link in the network.

The impact of these variances is that the control environment over identical IT infrastructure components can differ significantly. When considering IT infrastructure, a computer auditor may come across a wide range of environments, configurations, hardware and software. As ever, risk should be the critical factor in determining the amount of audit effort required and the most effective audit approach to be adopted.

4.3 Infrastructure Areas

The following areas are of interest to the computer auditor in considering IT infrastructure, although the amount of work required under each heading will vary. For example, a physical security review of a purpose built computer centre housing a large IBM mainframe computer may require a specific audit of several weeks duration. A review of the physical security aspects of a user based PC, however, may only, require a few hours work and could be incorporated into a larger scope audit.

4.3.1 Physical Security

Accidental or deliberate physical damage to IT equipment could damage the software and data of the organisation. Given the large capital investment made by organisations in IT, not only could this result in a significant financial cost to the organisation, but also the non-availability of the system could have a major impact on the well-being of the organisation. It is essential that effective physical security arrangements are in place to protect the IT environment from accidental or malicious damage.

The term physical security can be further considered under the following headings:

Physical Access

This is concerned with restricting access to IT infrastructure to authorised persons only. Physical access will initially consist of perimeter security which may be achieved by the use of walls and fencing, supported as appropriate by such controls as CCTV or security guards. Within the building, various IT infrastructure components such as telecommunications and central processing units should be segregated and an access control system should be installed to restrict the access of unauthorised personnel. Typically, this will involve some form of card based access control system, although more sophisticated systems using biometrics, such as finger print scanning may be found. Comprehensive intruder detection systems, incorporating a combination of contact breakers and passive infra red detectors should be used, connected directly to a central monitoring station.

Fire Protection

Fire represents a key area of risk to IT infrastructure and good fire protection systems are essential. Fire protection is generally considered under the following headings:

- **fire prevention systems** - these include no smoking policies, good housekeeping practices such as the prompt removal of waste paper or the use of fire proof materials
- **fire detection systems** - these include the use of smoke and fire detectors in ceiling and floor voids and manual fire alarms, which should be connected directly to a central monitoring station
- **fire extinguishing systems** - traditionally Halon has been used as an effective extinguishing agent although environmental concerns mean that this is no longer appropriate. Other types of extinguishing system include CO2 and fine spray water sprinkler systems. The systems should be capable of manual and automatic activation and also be linked to an automatic power down of the IT equipment

Power Supplies

The availability of quality power supplies is essential to the efficient running of IT infrastructure, otherwise data corruption and equipment damage can occur. A wide range of devices are available to smooth out potential fluctuations in the quality of the power supply, known as spikes and troughs, such as an uninterruptable power supply (UPS) system. Again, dependent on risk, it may also be appropriate to have a back-up power supply in the event of a mains failure. This will usually consist of a back-up generator and a short term battery powered supply.

Air Conditioning

As with power supplies, IT infrastructure is sensitive to its operating environment. Controls are needed to ensure the quality of air and the temperature. Typically, air conditioning systems will be installed, together with good housekeeping procedures, such as avoiding the shredding of paper in the vicinity of IT equipment.

Flood Protection

Flooding can be caused by both internal and external sources and the impact can be significant, particularly if the water is contaminated, in which case equipment may be damaged beyond repair. Water detection systems should be installed and where possible, water supplies should be routed away from IT equipment. Care should also be given to the siting of IT equipment so that it is protected from local hazards, such as being below ground level in an area prone to flooding.

Computer Audit Involvement in Physical Security

In considering physical security, the computer auditor should be aware that in some areas this can be a specialist field. In these circumstances, e.g. fire systems, computer auditors should seek the advice of specialist organisations such as the Fire Brigade. Careful risk analysis is necessary to determine the amount of audit work required in this area and to ensure that the level of control is commensurate with the degree of risk to the organisation.

The computer auditor should ensure that effective security and control mechanisms are in place so that the computer installation is physically secure and is adequately protected against potential destruction and physical loss. Audit work will rely heavily on observation and discussion, together with a review of available documentation such as access control logs, and associated manual procedures, such as those for allowing access to visitors.

4.3.2 Contingency Planning

Such is the dependence on IT by an increasing number of organisations that the non-availability of their IT infrastructure could have a profound impact on the well being of the organisation, if not on its continued survival. Research has indicated that of those organisations suffering a major IT failure, the majority will be out of business within two years.

Effective physical security controls can do much to prevent or restrict the potential impact of a disaster, but it is essential that effective and tested contingency plans are in place to enable the organisation to survive such an eventuality. Contingency plans should cater for various levels of IT infrastructure failure, from strike action by key IT staff, to a major disaster such as a fire or flood which completely destroys the IT capability.

In terms of larger IT installations, a number of different strategies can be adopted for contingency. These include:

- **hot standby** - a dedicated site is available to resume processing from the main site almost instantaneously. This site will have identical IT hardware, software and data to the main site
- **warm standby** - an alternative, similarly configured site is available to resume processing, but which will require several hours to set up, e.g. to load back-up data. Typically, these sites are provided by specialist disaster recovery services such as CDR (Computer Disaster Recovery) or Guardian Computer Services and may be shared by several users
- **cold standby** - where premises are available which must first be equipped out with hardware, etc. before they can be used. Typically these range from an empty warehouse to a spare office or a portacabin
- **reciprocal agreements** - arrangements with other organisations operating similar equipment are also an option, although in reality, these tend to be impractical in today's IT dependent business environment

Clearly the specific needs of the business will determine which is the most appropriate solution to its needs. For smaller IT environments, variations of these strategies can be adopted.

It is important to ensure that IT contingency plans do not exist in isolation of the business. Business requirements, ideally in the form of a wider business resumption plan, should be clearly identified and should provide the basis for subsequent contingency planning. Regular and thorough testing of the plan is essential if an assurance is to be obtained as to its effectiveness. IT is such a dynamic area and regular testing helps to ensure that potential problems are identified and resolved.

Computer Audit Involvement in Contingency Planning

Ideally, computer auditors should be involved in the development of a contingency plan and in the testing process. The objective of this involvement is to ensure that the plan is comprehensive, up to date, and meets the requirements of the business. The computer auditor should consider whether a contingency plan exists and if it is documented, up to date and regularly tested. Areas to consider include ensuring that the correct back-ups are taken, stored off-site and that the back-up hardware and software environment will meet the needs of the business.

4.3.3 Logical Access Control

The nature of IT is such that the emphasis of the traditional control environment has moved to one of prevention rather than detection. Most organisations now use on-line or real time systems where data is updated and transactions are initiated immediately. Logical access controls, therefore, are a key feature of IT infrastructure in that they provide the ability to identify and authenticate users and thereby control access to and usage of the system.

The basic purpose of logical access controls is to restrict authorised users to performing authorised activities from authorised locations via only authorised channels. It is essential, to achieve an effective balance between having too much security and allowing too much flexibility and access for the users.

In operating systems such as VMS from DEC, Windows NT from Microsoft and OS/400 from IBM, security functionality is integrated within the operating system software. In others, such as the large IBM operating system, MVS, separate logical access control software will have to be implemented to achieve the required level of security - Top Secret and ACF2 from Computer Associates and RACF from IBM are the most common packages available for this purpose. In some operating systems, notably the various flavours of UNIX, security functionality is included within the operating system software, but it may need to be supplemented by third party packages such as BOKs, to achieve the required level of security.

The basic components of logical access control systems include:

- **environmental controls** - where system-wide options/parameters are set. These include the initial security level, whether protection is to be extended to magnetic media, password options such as the number of invalid attempts allowed and the enforcement of password changes
- **user controls** - where restrictions are put on who can access the system and from where. Usually, there will be a number of users in the system who are privileged; that is they have

special attributes which enable them to perform special actions. In UNIX, for example, the privileged user is known as “Root” and has access to all system resources

- **resource controls** - where the protection for resources such as databases are created, e.g. when is access to this database to be allowed, is the access to be read only and from what terminal?

Logical access control systems can be customised although this can have a significant effect on the security of the IT system. The customisation is achieved by a series of parameters or values which determine how the software will work, e.g. how many logon attempts will a user be allowed? Exits are also included which enable an organisation to develop its own logical access controls code.

The administration of logical access control is particularly important. Specifically, it is advisable to segregate the administration of logical access control from other operational activities and to provide for regular checking of the administrator’s activities, e.g. the independent review of audit trails.

A key issue of logical access control is that with the proliferation of IT systems, many users are required to hold several User-IDs and passwords. Inevitably, this results in users keeping a record of them, so compromising security. It is technically feasible to implement a single sign-on system where a user is authenticated at the point of entry and only has to sign-on once. Such systems, however, do not necessarily provide for a secure single sign-on as frequently, passwords are distributed in clear text. There are problems of password synchronisation and, invariably, the available products do not cater for all of the IT platforms that an organisation is likely to use.

Computer Audit Involvement in Logical Access Control

The basic objective of a logical access control review is to establish whether controls over access to systems, data, software and resources are adequate. Ideally, the computer auditor should be involved in the initial design of the access control system when appropriate advice and guidance on the level of security can be provided.

The computer auditor should review the access control administration function to ensure adequate segregation, procedures and checking of work. The system-wide options and locally coded exits should be reviewed to ensure that they do not compromise security. Limited testing may be undertaken to ensure that key databases and system resources are sufficiently protected and that user’s access rights are consistent with their operational duties. An important consideration is to ensure that effective mechanisms have been established to investigate potential and actual breaches of IT security.

4.3.4 Change Control

Change is a common feature of the IT world. It is important that effective control procedures are in place to ensure that only authorised changes are made to IT systems. Not only is there scope for the accidental or deliberate inclusion of unauthorised code (the so called Trojan horse or time bomb) but change involves a degree of risk and it is necessary to ensure, for example, that the right version of software is actually implemented.

Formal change control systems are necessary to ensure that changes to application software, systems software, and even IT hardware, are adequately tested, authorised and moved to live production in a controlled manner. A variety of change control software products are available to assist, notably CA-Librarian and Endevor for IBM systems. Many operating systems include basic change control functionality, whilst a number of organisations develop their own to meet specific needs. The basic functions of this software are to:

- establish different logical environments for programming, testing, quality assurance and live program versions
- restrict access to program code
- provide version control over the program libraries
- provide an audit trail facility

Formal change control systems should accommodate not only scheduled changes, but also the need for emergency changes, whether they be software or data. The basic principles of change control apply to emergency changes, i.e. authorisation is required, although detailed investigation, testing and documentation of the change may be undertaken after the event.

Computer Audit Involvement in Program Change Control

The objective of the computer auditor is to obtain an assurance that changes to applications and systems software and hardware are adequately controlled. The computer auditor should ensure that a change control system is in place which accommodates both scheduled and emergency changes. An assurance should also be obtained that an authorisation mechanism is in place, that adequate documentation of the change is produced, that the integrity and security of program versions is maintained and that the implementation process provides for back-out routines.

4.3.5 Operating Systems

An operating system is usually defined as a set of programs which permit the continuous operation of a computer. The software controls scheduling and execution of application programs and use of computer resources. Simplistically, the operating system acts as the interface between the application program, the user and the IT hardware. The security and control of an operating system is a complex issue and provides an area of potentially major risk to an organisation.

The complexity, size and functionality of operating systems varies enormously from one manufacturer to another. Some operating systems may include functionality, such as database management systems and security software, whilst others will require separate systems software to perform such tasks.

Some of the most well known operating systems include MVS from IBM, which contains over 10 million lines of code, VMS from DEC and VME from ICL. Whilst operating systems such as MVS, VMS and VME are proprietary to that manufacturer and dependent on its hardware, a few operating systems, notably UNIX, are portable and can be run on a range of manufacturers' hardware. This portability, however, may be limited, as invariably basic UNIX is customised by each supplier to provide its own features, such as AIX from IBM and HP-UX from Hewlett Packard. In effect, these portable, or open systems, become proprietary and dependent on a specific manufacturer's hardware.

The extent to which operating systems need to be customised varies considerably, not only from one operating system to another, but from organisation to organisation, depending upon its specific requirements. Usually, most operating systems will have a series of parameters or values which determine how the operating system will work. Exits are also included which enable an organisation to develop its own operating system code. This customisation can have a significant effect on the confidentiality, availability and integrity of IT processing.

In larger organisations, running large complex operating systems, it is not uncommon to have personnel specifically responsible for fine tuning and customising the operating system. Effective control procedures are required over such personnel.

Computer Audit Involvement in Operating Systems

The audit of operating systems is a complex and time consuming area. In some instances, software is available to assist in this process, such as CA-Examine for MVS.

The basic objective of the computer auditor is to ensure that the security and integrity of the operating system has not been compromised. The auditor should consider whether responsibility for the maintenance of the operating system has been established and that suitable procedures have been documented. An effective change control system is necessary to ensure that only authorised amendments can be made to the operating system. The computer auditor should also ensure that system initiation procedures are established to prevent unauthorised changes.

4.3.6 Telecommunications

The major development in computing in the last few years has been the rapid expansion of telecommunications. As a result, a vast amount of data is regularly transmitted throughout the world and with it there are significant security and control exposures, specifically in terms of availability and integrity.

There are many different types of telecommunications networks, such as local area networks (LANs) which are usually confined to individual offices and wide area networks (WANs) which can span continents. Telecommunications software is necessary to operate these networks and to enable communication between user terminals and the application program. A vast array of network protocols are necessary and several will be found in the same organisation, whether for historical or specific business reasons (a protocol is a set of standards to ensure data moves efficiently around a network). Typical protocols include IBM's SDLC Synchronous Data Link Control and TCP/IP (Transmission Control Protocol/Internet Protocol).

Telecommunications software typically provides the following functionality:

- controlling the flow of data in a network
- providing for recovery and resilience
- MIS on network performance and capacity management
- security and cryptography functionality
- network administration tools
- network audit trails

Again, telecommunications is a very specialised area possibly requiring the support of a separate team. The number of staff required will vary from installation to installation, and may comprise several sections in large organisations running software such as IBM's SNA (Systems Network Architecture).

As with operating systems, telecommunications software can be customised as appropriate by an organisation. Exit points are also available to enable user code to be implemented. Some telecommunications software, such as CICS (Customer Information Control System) also includes security software features.

Computer Audit Involvement in Telecommunications

The basic audit objective is to ensure that adequate security and control is in place over the organisation's telecommunications networks. Initially, the computer auditor must obtain network diagrams of all physical and logical connections. The computer auditor should ensure that telecommunications hardware, such as front-end processors (FEPs) are physically secure. Effective control should be exercised over the addition or deletion of devices to the network and documented procedures should govern the work of the various personnel involved in the network. The computer auditor should assess the adequacy of the back-up arrangements and assess whether adequate control is exercised over the use of diagnostic tools, such as datascopes which could compromise network integrity or confidentiality. Particular attention should be paid to the existence of any dial-in connections.

4.3.7 Cryptography

The risks associated with the transmission of data over extensive telecommunications networks (parts of which may not be under the organisations direct control) have created a need to take additional steps to prevent the unauthorised/accidental corruption of messages in transit, or a breach of confidentiality. Cryptography can be used to ensure confidentiality, integrity, non-repudiation and authenticity and includes such techniques as encryption and digital signatures. Military organisations and banking institutions make extensive use of cryptography.

Encryption

Encryption is a widely used technique which involves making information indecipherable to protect it from unauthorised viewing or use, especially during transmission or when it is held on removable magnetic media. Encryption is usually based on a key(s) without which the information cannot be decoded (decrypted). The most widely used encryption system is DES (Data Encryption Standard) although increasingly this is being replaced commercially by the more secure public key system RSA.

Message Authentication

Message authentication makes use of encryption to create a digital signature which is appended to a transaction. This does not scramble the data but any difference in the digital signature at the receiving end will indicate some form of message corruption.

Computer Audit Involvement in Cryptography

Cryptography is a very specialised and complex area and a review of this requires a high degree of specialised knowledge. Typically, in ensuring that adequate controls are in place over authentication and encryption, the computer auditor will wish to ensure that encryption hardware is physically secure, that audit trails are made of key change activity and that the generation of keys is well controlled.

4.3.8 Computer Operations

Within any type of computer installation, personnel are required to operate the IT systems. The tasks undertaken, the number of personnel required and the extent of automation involved may vary significantly from one installation to another. Typical operating tasks include:

- job scheduling
- operating IT hardware

- housekeeping
- recovery and back-up

Computer Audit Involvement in Computer Operations

The basic objectives of the computer auditor are to assess whether adequate controls are in place over data preparation, the completeness of processing and the dispatch of output. The computer auditor will wish to ensure that adequate audit logs of operator activity are maintained, that the computer room is tidy, that there is an adequate segregation of duties and that work is appropriately organised. The computer auditor should also ensure that output is securely controlled and that appropriate arrangements exist for re-runs and that unwanted output is safely disposed of.

4.3.9 Databases

A database may be defined as "a collection of inter-related data which is organised so that, as far as possible, it is independent of any specific application and wherever possible, not duplicated". A database is a structured way of storing and managing data in a consistent manner, which is independent of the physical structure of the data. Data is arguably one of the organisation's most important resources and as such it is essential that strong controls are in place over its use.

There are two main types of database:

- **hierarchical or CODASYL -** hierarchical databases have a "tree" structure, with a hierarchy of nodes, the top node being the "root" node. One of the most common examples of this type of database is IMS (Information Management System) from IBM
- **relational -** with relational databases, data is modelled into logical records and relationships as before, but entities become rows in a table and attributes become columns. DB/2 from IBM is an example of a widely used relational database

The database which holds the data is controlled by software known as a database management system (DBMS). The purpose of this system is to manage the data in the most efficient form. All requests to read, change, insert or delete data must be made through the database management system. Logs are also maintained of such actions. Usually, the database management system incorporates security software to control access to the data.

Computer Audit Involvement in Databases

The basic objective of the computer auditor is to assess the integrity and availability of the database. Key areas of interest are to restrict access and to ensure a satisfactory segregation of duties between the database administrator and other operation and support functions. Local exits should be reviewed, together with the various DBMS options to ensure that security has not been compromised.

4.3.10 Storage Media

Most organisations operating sophisticated IT systems will hold a vast quantity of data. In general, this will be held on direct access storage devices (DASD) such as fixed disks. In some instances, notably archive data and back-up data, other media such as cartridges, magnetic tapes or optical disks may be used. Often, robotic devices such as cartridge libraries are in use to automate the control of such media, although manually administered tape libraries will also be found.

The concentration of such a quantity of data in a small number of locations poses potential risks to an organisation. It is essential, therefore, that this data is held securely, that it is protected from unauthorised use and that adequate records of its use are maintained. Specific procedures are required to provide for the safe disposal of magnetic media, for which devices such as degaussers may be used.

Computer Audit Involvement in Storage Media

The computer auditor should ensure that satisfactory control is exercised over its use and storage and that it is physically protected from accidental or deliberate damage. The computer auditor should determine what data is held on magnetic media and its significance to the organisation. There will be a need to ensure that authorisation mechanisms are in place for the use of media and that procedures provide for its correct labelling and cleaning.

5. Audit Automation

5.1 Background

In many organisations, the origins of computer audit lie in the need for business auditors to obtain independent data from the system and subsequently, to obtain an assurance about the internal workings of the IT system. Although audit automation still represents a core activity of many computer auditors, increasingly, this activity is being transferred to business auditors. This transition has been facilitated by the availability of more user friendly application software. The role of the computer auditor in this environment is to provide specialist expertise to the business auditors, rather than perform the activity.

IT can deliver significant benefits to the audit process in terms of: timeliness, efficiency, professionalism and increased productivity.

Audit automation is generally considered under two main headings:

- as an audit tool
- as an administration tool

5.2 Audit Tools

Audit automation, in this context, involves the use of computer assisted audit techniques (CAATS) as an integral part of an audit review to increase its overall efficiency and effectiveness. CAATS are generally categorised into those which review data and those which review controls.

Those CAATS which review data generally involve the extraction, examination and manipulation of data by programs. Such techniques can enable the auditor to gain an assurance as to the accuracy and integrity of the data being reviewed and, by implication, the strength or weakness of control. Those CAATS which review controls look at the system rather than data and provide the auditor with an assurance as to whether or not controls exist and are functioning effectively. By implication, this will cause the auditor to question the accuracy and integrity of that data.

Traditional text books on computer audit usually refer to a large range of CAATS. Although some of these are used to varying degrees by some organisations, in practice, interrogation software is the most widely used CAAT.

5.2.1 Interrogation Software

Interrogation software involves the production of a computer program to interrogate either system or application data. Standard programming languages such as COBOL may be used and generalised audit software is also available from the accounting firms, such as System 2190 from KPMG. Specific retrieval software such as Easytrieve from SRA can also be obtained. Increasingly, there is a large range of third party software products available for the development of CAATS. Some of the most widely known include:

- IDEA (Interactive Data Extraction & Analysis)
- ACL (Auditor Command Language)
- SQL (Structured Query Language - used with relational databases)
- SAS (Statistical Analysis Software)

There is also a wide variety of other third party software which can assist in an audit review, such as CA-Examine for a review of the IBM MVS operating system, or the Enterprise Security Manager from Axent for a review of UNIX.

5.2.2 Embedded Data Collection

This is similar to interrogation software, but the program logic is embedded within the live application program or systems software.

5.2.3 Parallel Simulation

This involves the re-writing of a system and processing data through it so that the results can be compared to the live system.

5.2.4 Others

There are a variety of other tools, such as code comparison software which can compare two files, containing either data or program code, and highlight differences.

5.3 Administration Tools

A large range of products is now available to assist in the effective running of the internal audit function. These can be developed in-house or acquired from third party suppliers. In some instances, such as planning software, generally available products such as PMW can be used, although audit specific products are increasingly becoming available. Not only do such products simplify the administration of the function, but they also provide a more professional service for the organisation.

Typically products will be used for such areas as: planning, risk assessment, time recording, electronic working papers and presentations.

Glossary of Terms

The following glossary is designed to give readers an understanding of some of the more common acronyms which will be found in the computer auditing arena.

ACF2 : An access control software product for mainframe computers, produced by Computer Associates

AIX : The IBM version of the UNIX operating system

Application : A program which performs business functions such as payroll

ASCII : American Standard Code for Information Interchange - a code for representing characters in binary

Assembly Language : A low level language where one programming instruction corresponds to one machine code instruction

BS7799 : The British Standard Code of Practice for Information Security Management

C : Programming language closely associated with UNIX

CAD : Computer Aided Design

CAM : Computer Aided Manufacturing

CASE : Computer Aided Software Engineering

CD-ROM : Compact Disk - Read Only Memory - large capacity storage media using compact disks of varying sizes. These are read only

CICS : Customer Information Control System - IBM product that enables transactions entered at remote terminals to be processed concurrently by user written application programs

Client Server Architecture : LANs that make use of distributed intelligence to treat both the server and the workstations as intelligent programmable devices

COBOL : COmmon Business Orientated Language - high level English-like programming language

Compile : Process of preparing a "machine language" program from a source language program such as COBOL

CP/M : A range of operating systems based on the Intel microprocessors from Digital

CPU : Central Processing Unit - main intelligence of the computer which processes instructions for execution

CRAMM : Computerised Risk Analysis and Management Methodology - a risk assessment methodology

Database : A collection of inter-related data which is organised so that, as far as possible, it is independent of any specific application and wherever possible, not duplicated

DASD : Direct Access Storage Device

DB/2 : A relational database management system from IBM

DBMS : Database Management System

DES : Data Encryption Standard - widely used encryption standard

DIP : Document Image Processing - scanning of documents onto optical disk

EBCDIC : Extended Binary Coded Decimal Interchange Code - a code for representing characters in binary

EDI : Electronic Data Interchange - transfer of electronic trading information through computer to computer communication

EFT : Electronic Funds Transfer - transfer of electronic funds through computer to computer communication

Ethernet : Local area network using a bus topology

Expert System : Application program that solves problems by using analytical rules and knowledge

FAST : Federation Against Software Theft - an organisation of vendors who work to eliminate software theft

FORTRAN : FORmula TRANslator - the first high level computer programming language used primarily in engineering and scientific environments

GUI : Graphical User Interface - pictorial representation of commands, files etc.

HP-UK : A version of the UNIX operating system from Hewlett Packard

Ingress : A relational database product

Internet : A global network of networks connecting a range of organisations

ISDN : Integrated Services Digital Network - a network that allows voice transmissions to be mixed with data and video services

LAN : Local Area Network - a group of computers and other devices spread over a relatively limited area and connected by communications links

MAN : Metropolitan Area Network - typically operates with a discrete geographic location (i.e. a city)

MICR : Magnetic Ink Character Recognition - the recognition of characters on paper by detecting the magnetic code on characters

Modem : Device that converts digital signals to analogue and vice versa to enable computers to communicate across telephones lines

MS-DOS : Microsoft-Disk Operating System - single tasking, single user operating system

MVS : Multiple Virtual Storage - IBM mainframe operating system

OCR : Optical Character Recognition - the recognition of printed characters on paper by detecting patterns of dark and light

OOP : Object Orientated Programming

Operating System : The software responsible for controlling the allocation and usage of hardware resources such as memory and CPU

Oracle : A relational database product

OS/2 : A protected mode, virtual memory, multitasking operating system from IBM based on the Intel x86 processors

Pascal : Concise procedural programming language

PMW : Project Manager Workbench - a project management tool

PRINCE : Project in Controlled Environment - a project management methodology

RACF : Resource Access Control Facility - an access control software product for mainframe computers, produced by IBM

RAD : Rapid Application Development - a development process to speed up the development of IT systems

RISC : Reduced Instruction Set Computing - a type of microprocessor that focuses on processing a relatively small set of instructions rapidly, rather than handling a much wider array of instructions

ROM : Read Only Memory - semiconductor based memory that contains instructions or data that can be read but not modified

RSA : Public key encryption standard

Server : On a LAN, the computer running the administrative software that controls access to all or part of the network and its resources

SSADM : Structured Systems Analysis and Design Methodology - a systems development life cycle methodology

Structured Query Language (SQL) : A database tool used to interrogate, update and manage relational database

Sybase : A relational database product

TCP/IP : Transmission Control Protocol/Internet Protocol - a set of standards for telecommunications

Token Ring Network : A network topology that uses token passing as a means of regulating traffic on the line

Top Secret : An access control software product for mainframe computers, produced by Computer Associates

Trojan Horse : An apparently useful program that contains hidden code, usually damaging

Ultrix : A version of the UNIX operating system from Digital

UNIX : A multi-user, multi-tasking operating system. Written in C it is more portable and less machine specific than other operating systems. The main versions are System V from AT&T and BSD from the University of California, Berkeley

UPS : Uninterruptable Power Supply - equipment to smooth out variations in the quality of the electricity supply

Virus : A program, usually harmful, that infects files, usually by inserting copies of itself in those files

VME : Operating system from ICL

VMS : Operating system from Digital

VTAM : Virtual Telecommunications Access Method - an IBM product to provide mainframe communication

Windows : A multi-tasking graphical user interface environment from Microsoft that runs on MS-DOS based PCs

WORM : Write Once Read Many - a high capacity read only storage device using optical disk

BARCLAY SIMPSON
Hamilton House, 1 Temple Avenue, Victoria Embankment, London EC4Y 0HA.
Tel: 0171 936 2601 Fax: 0171 936 2655 http://www.barclaysimpson.co.uk