Information Technology Audit

General Principles

Introductory

As computer technology has advanced, Government organisations have become increasingly dependent on computerised information systems to carry out their operations and to process, maintain, and report essential information. As a consequence, the reliability of computerised data and of the systems that process, maintain and report these data are a major concern to audit. IT Auditors evaluate the reliability of computer generated data supporting financial statements and analyse specific programs and their outcomes. In addition, IT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

IT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively, and uses resources efficiently. Data integrity relates to the accuracy and completeness of information as well as to its validity in accordance with the norms. An effective information system leads the organisation to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. IT Auditor must know the characteristics of users of the information system and the decision making environment in the auditee organisation while evaluating the effectiveness of any system.

Use of computer facilities has brought about radically different ways of processing, recording and controlling information and has combined many previously separated functions. The potential for material systems error has thereby been greatly increased causing great costs to the Organisation, e.g., the highly repetitive nature of many computer applications means that small errors may lead to large losses. An error in the calculation of Income Tax to be paid by employees in a manual system will not occur in each case but once an error is introduced in a computerised system, it will affect each case. A bank may suffer huge losses on account of an error of rounding off to next rupee instead of nearest rupee. This makes it imperative for the auditor to test the invisible processes, and to identify the vulnerabilities in a computer information system as the costs involved, because of errors and irregularities, can be high.

Controls in a Computer System

Computer systems are efficient and achieve results accurately and at great speed if they work the way they are designed to. They have controls provided to ensure this but the controls have to be effective. The controls are of great value in any computerised system and it is an important task for an auditor to see that not only adequate controls exist, but that they also work effectively to ensure results and achieve objectives. Also controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels.

Controls in a computer information system reflect the policies, procedures, practices and organisational structures designed to provide reasonable assurance that objectives will be achieved. The controls in a computer system ensure effectiveness and efficiency of operations, reliability of financial reporting and compliance with the rules and regulations.

Information system controls are broadly classified into two broad categories:

- General Controls
- Application controls

General controls include controls over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. They create the environment in which the application systems and application controls operate. Examples include IT policies, standards, and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, service continuity planning, IT project management, etc.

Application controls pertain to specific computer applications. They include controls that help to ensure the proper authorisation, completeness, accuracy, and validity of transactions, maintenance, and other types of data input. Examples include system edit checks of the format of entered data to help prevent possible invalid input, system enforced transaction controls that prevent users from performing transactions that are not part of their normal duties, and the creation of detailed reports and transaction control totals that can be balanced by various units to the source data to ensure all transactions have been posted completely and accurately.

Significance of controls

Presence of controls in a computerised system is significant from the audit point of view as these systems may allow duplication of input or processing, conceal or make invisible some of the processes, and in some of the auditee organisations where the computer systems are operated by outside contractors employing their own standards and controls, making these systems vulnerable to remote and unauthorised access.

Apart from this, the significance of controls lies in following possibilities:

(i) data loss due to file damage, data corruption (manipulation), fire, burglary, power failure (or fluctuations), viruses etc.

(ii) error in software can cause manifold damage as one transaction in a computer system may affect data everywhere;

(iii) computer abuse like fraud, vengeance, negligent use etc. is a great potential danger and

(iv) absence of audit trails make it difficult for an auditor to ensure efficient and effective functioning of a computerised system.

Objectives of Computer Controls

The objectives of controls do not change with the introduction of computers. It is the control techniques that change with many of the manual controls being computerised and new technical computer controls added to achieve the same objectives. Typical control objectives within a government Data Processing function are to ensure:

(i) provision of effective organisational control over functions related to Data Processing by clearly defining organisational objectives;

(ii) effective management control over development of Data Processing resources in accordance organisational objectives;

(iii) practices related to Data Processing activities in accordance with statutory requirements and down administrative procedures;

(iv) formulation of an adherence to policies, standards and procedures for all functions related to Data Processing and

(v) efficiency and effectiveness of the Data Processing systems towards achievement of its desired objectives.

Preliminary evaluation

The first step in audit should be preliminary evaluation of the computer systems covering:

(i) how the computer function is organised.

(ii) use of computer hardware and software,

(iii) applications processed by the computer and their relative significance to the organization and

(iv) methods and procedures laid down for implementation of new applications or revision to existing applications.

In course of preliminary evaluation, the auditor should ascertain the level of control awareness in the auditee Organisation and existence (or non-existence) of control standards. The preliminary evaluation should inter alia identify potential key controls and any serious key control weaknesses. For each control objective the auditor should state whether or not the objective has been achieved; if not, he should assess the significance and risks involved with due to control deficiencies.

Audit methodology

After completing the preliminary evaluation of the computer systems, the auditor has to decide about the appropriate audit approach, system based or direct substantive testing. In doing so, the aspects to be borne in mind are:

(i) results of the preliminary evaluation

(ii) extent to which reliance can be placed on any work carried out by Internal Audit and

(iii) nature of any constraints like lack of any audit trail and the practicability of testing.

(iv) effective compliance testing of key computer controls (which may be difficult) and

(v) each control to be tested will require large samples.

A Direct Substantive Testing

If Direct Substantive Testing approach is chosen, a sample of transactions should be selected and tested. Result of the preliminary evaluation will be of help particularly as it would have:

(i) provided an overall assessment of the control environment and identified any serious weaknesses which should be raised with the auditee,

(ii) given sufficient familiarity with the system to be able to decide the point from which to select the transactions for testing and how to substantiate them efficiently and

(iii) provide sufficient information to determine any initial requirement for any CAATs.

B Systems Based Audit

For System Based Audit approach, aspects of regularity, economy, efficiency and effectiveness of the system have to be looked into besides evaluating data integrity, and data security as explained below:

(i) System effectiveness is measured by determining whether the system performs the intended functions and whether users get the needed information, in the right form when required;

(ii) A system is economical and efficient if it uses the minimum number of information resources to achieve the output required by the users. The use of system resources - hardware, software, personnel and money - should be optimized;

(iii) System activities would be regular if they comply with applicable laws, rules, policies, guidelines etc;

(iv) Achieving data integrity implies that the internal controls must be adequate to ensure that error are not introduced when entering, communicating, processing, storing or reporting data; and

(v) Data system resources, like other assets, must be sufficiently protected against theft, waste, fraud, unauthorized use and natural disasters.

The key controls for ensuring the above will have to be identified, recorded, evaluated and compliance tested. The result of the preliminary evaluation would be of help particularly as they would indicate system deficiencies, major weaknesses and the areas requiring in-depth study. Identification of key controls would also depend on experience of the auditor gained in course of audit of similar installations.

Compliance testing of controls in computer systems and programmes is difficult and complicated as their operation is automatic, invisible and not fully evidenced (only the exceptions are normally evidenced). Detailed manual testing of these controls is rarely cost effective, but a possible alternative approach is to use a CAATS. For example, either test data or audit software may be used to test a control which is designed to ensure that payments exceeding a certain value should not be made.

Audit software can be used to interrogate the whole payments file to identify any payments which exceeded the specified value. If no such cases are revealed, the auditor has some, assurance in that no such payment was made. This is a negative assurance since it is possible that no invalid data was in fact presented to the system (and hence the control was never invoked). However, if the interrogation is applied to the whole year's transactions, it achieves the main audit objective in that no excessive payments will have been made in the period.

Even when test packs or interrogation are used, the auditor should examine the procedures for dealing with exception or error reports, to ensure that invalid transactions are corrected and re-input for processing.

Audit techniques

IT audit techniques refer to the use of computers, including software, as a tool to independently test computer data of audit interest. Some well-established techniques are:

(i) collecting and processing a set of test data that reflects all the variants of data and errors which can arise in an application system at different times;

(ii) using integrated test facilities, built into the system by the auditee to help the auditor in his requirements, as one of the users of the system;

(iii) simulating the auditee's application programs using audit software to verify the results of processing;

(iv) reviewing program listings periodically to see that there are no unauthorised alterations to the programs;

(v) using either commercial software or in-house developed programs to interrogate and retrieve data applying selection criteria and to perform calculations and

(vi) extracting samples of data from the auditee database/files, using sampling techniques, for post analysis and review. The nature of data and type of analysis required determine what technique is to be employed. The auditor should give the sample size and design.

Computer audit techniques are employed for:

(i) verification of ledger balances and control totals independently,

(ii) recalculation of critical computerised calculations to check mathematical correctness;

(iii) range checks to verify the working of computer based controls and testing for exception conditions;

(iv) testing the validity of data which have gone into the master file

(v) detection of data abuse/frauds and

(vi) substantive testing with large volumes of data which is difficult, if not impossible, in a manual audit process.

The particular computer audit technique employed depends on:

(i) the type of application system under review;

(ii) the extent of testing required;

(iii) the availability of resources in terms of computer facilities, and the level of EDP skills among the audit staff; and

(iv) Volume of data and availability of printer information

Where data volume is small and adequate printed information is available to carry out a meaningful clerical audit, there is no need to employ computer techniques, which are costly and time consuming. To elaborate further, the auditor should break up his project of application system audit into three stages. In the first stage, he will carry out the examination of audit trails, intermediate printouts as required, system logs and operational controls. As a result of audit in the first stage, if the auditor feels that the adequacy of controls requires further verifications, in the second stage he can carry out compliance testing by using the test deck method and integrated test facilities with resident audit programs. If the compliance testing exposes some control weaknesses, substantive testing may be resorted to in the third and final stage using retrieval software and simulation techniques with audit software.

Today, many DBMSs have built-in query and report writer facilities. Unstructured queries on the data files are also possible in some advanced systems. These utilities could be profitably employed for audit purposes. The auditor will be able to obtain the relevant information from the auditee's computer centre.

The distinct advantages of retrieval packages over other methods are 100 per cent review of data and accuracy of processing and effective use of the auditor's time in analysing results of Interrogation. Use of retrieval software will, however, always remain a problem area primarily because of the multitude of hardware and software systems in use in various departments, necessitating expertise in several programming languages.

Main Points to be checked in different Audit Areas

Audit of Acquisition

Generally the acquisition of computer facilities involves the following stages:

(i) definition of a computer policy and strategy (evaluation of organisational requirements and the ways and means of satisfying them);

(ii) establishing the need;

(iii) a thorough examination and evaluation of the alternative courses of action available;

(iv) specifying precisely the requirements (delineating existing and future applications, hardware, software, modes of operations, conditions of supply, etc.);

(v) evaluating the alternative sources of supply and selecting the most appropriate source(s), and;

(vi) physically acquiring the facilities and the systems.

Often these stages tend to overlap or merge imperceptibly, into one another.

Acquisition of computer facilities may include:

(i) acquisition of hardware involving

(a) introduction of a completely new installation,

(b) enhancement of central processor,

(c) enhancement of peripherals,

(d) addition/replacement of a specific equipment and

(e) introduction of several small computers.

(ii) acquisition of software involving

(a) general software associated with changes in hardware (a new operating system),

(b) specific purpose software and

(c) ‘off the shelf' application software.

The auditor has to review the adequacy of administrative procedures and controls used by the auditee oganisation when considering and deciding upon the acquisition of computer facilities. For this purpose, he has to see that:

(i) a sound administrative structure exists to produce a proper analysis of the requirements of computer facilities:

(ii) the acquisition procedures are effective in producing a viable computing policy and strategy and

(iii) the process of evaluation and selection ensure that the requirements of the Organisation are met in the most effective and efficient way - sufficient and adequate disposal.

The auditor should direct his attention to the following areas:

(i) EDP policy and strategic plan;

(ii) administrative structure;

(iii) feasibility study / project report containing proposals, costs and benefits; equipment selection

(iv) justification for hardware and software;

(v) installation of equipment and adequacy of testing and

(vi) post implementation review and costs.

Feasibility study report should cover points like clear statement of objectives, existing arrangements, alternative solutions, proposed solutions, financial implications and schedule of implementation. In case of equipment selection, points to be borne in mind are:

(i) specifications of requirements for acquisition, enhancement or replacement of computing facilities are stated concisely and precisely (as they form the basis for potential suppliers);

(ii) both technical and commercial aspects of the proposal are evaluated according to standard contracting procedures and

(iii) procurement action is taken after ensuring that the suppliers' offers meet the requirements of the specifications by taking into account inter-alia (i) technology options available at the time of procurement, (ii) useful life of the asset, (iii) incidental costs which could eventually be of sufficient magnitude, besides hardware and software costs and (iv) future development plans of the potential suppliers in terms of expendability, upgradability, etc.

Audit of Development

Since the underlying purpose of acquisition and development (designing, building or modifying) is the same, the audit concerns relating to acquisition, viz., planning, requirements definition, analysis of, alternatives and justification for the selected approach, are equally important in the review of systems development. Broadly stated, the audit objective of system development controls is to ascertain that procedures are adequate to ensure that the development results in well-documented computer systems incorporating adequate controls and meeting properly defined user requirements in an efficient manner.

There is also a need to examine the system testing and data transfer procedures as:

(i) inadequate system testing before line operation may result in the operation of a system which may not correctly process and record transactions and

(ii) inadequate data transfer procedure may result in the relevant records being inaccurately and incompletely transferred from the old to the new system.

Where systems development is entrusted to contractors, the contract and its management become important audit concerns. It should be ensured that the vendor provides complete documentation alongwith source code. Further, the terms and conditions like the rights over the source code provisions for modifications/updating in future should be examined. The penal provisions may also be examined in case of non-deliver of services/ non-adherence to time schedule. It may also be seen if any objectives could not be achieved due to delay in delivery of the software.

Categories of System Development Audit

System development audits can be categorised into three general classes:

(i) monitoring audits, in which the auditor evaluates the project throughout the process to determine whether development is proceeding effectively, e.g., whether milestones are being met, expenditure rates are as predicted, high quality documentation is being written, software conforms to established. technical standards, tests are being conducted as scheduled or evaluated as planned;

(ii) design review audits, in which the objective is to determine whether the preliminary and detailed designs accurately reflect the functional data and systems specifications, and incorporate adequate internal controls and

(iii) post implementation audits, performed three to six months after the system becomes operational, serve to evaluate whether the system meets requirements, is cost-effective and generally provides benefits predicted in project planning documents.

Association of audit in systems development

The ultimate responsibility for incorporating internal controls and an adequate trail into computer-based systems must rest with the auditee. The auditor therefore does not need to provide, as a matter of policy, any consultancy advice on developing systems. Nonetheless, audit should be aware of all developments which are likely to have significant impact on his audit. At an early stage in the design process of a new system, the auditor should consider providing the auditee with specific comment on:

(i) internal controls in the light of weaknesses identified in the existing system,

(ii) audit needs such as data retention or retrieval facilities and audit trail requirements and

(iii) any requirement which might enable him to carry out audit, or improve its efficiency and effectiveness.

Main points to be checked by Audit in System Development

While the auditor should be cautious enough not to be drawn into unproductive involvement in system development, the points that he should examine are the following:

(i) whether a published standard methodology is being used for designing and developing systems?

(ii) whether there is a common understanding by all parties-users, systems analysts, management and auditors-of the basic structure of both manual and computer processing activities, as well as of the concepts and needs for control and of the applicable control techniques? (This understanding must be reached first at a non-technical, user level)

(iii) Who authorises IT applications development – the user or steering Committee or management?

(iv) Whether the system development work was preceded by a feasibility study to determine the most appropriate solutions to standard problems?

(v) Whether there is adequate cross referencing between the following stages:

(a) content and format of preliminary studies,

(b) feasibility studies.

(c) system specifications,

(d) program coding

(vi) Whether project management techniques, are applied in system development work-that is to say, are there project decision milestones, time and cost estimates so that progress could be monitored against estimates?

(vii) Whether programming standards using modular structured methodology are being adhered to in coding?

(viii) Whether existing in house or external available application packages were considered before deciding upon new in-house application development?

Audit of Operation and Maintenance - General Controls

The auditor has to review the internal controls which are essential for proper operation and maintenance. Some of the operation and maintenance controls fall in the category of general controls relating to the whole set of computer facilities.

The overall audit objective in reviewing the general controls is to ensure that the controls and procedures are adequate to provide secure, effective and efficient day-to-day operation of the computer facilities. The controls and procedures which together form the general controls are discussed in the succeeding paragraphs.

Organisational controls

Such controls ensure that (i) there is judicious separation of duties to reduce the risk of employee fraud or sabotage by limiting the scope of authority of any individual, (ii) there are comprehensive written standards and (iii) access to and use of computer terminals is properly authorised.

These high level controls are important as they influence the effectiveness of any lower level controls which operate within accounting applications. Unless management maintains appropriate IT policies and standards, it is unlikely that other controls will be sufficiently strong to support a controls reliant audit approach.

An assessment of the high level IT policies, strategies and procedures will provide the auditor with a reasonably reliable indication as to the existence and effectiveness of any lower level detailed controls.

Segregation of duties

The auditor should check whether adequate and effective segregation of duties has been in place amongst the staff operating the computer system as it substantially reduces the risk of error and fraud. Poor segregation could lead to any one person, with control over a computer function, making an error or committing a fraud without detection.

Evidence of separation of duties can be gained by obtaining copies of job descriptions, organisation charts and observing the activities of IT staff. Where computer systems use security profiles to enforce separation of duties, the auditor should review on-screen displays or printouts of employees' security profiles in relation to their functional responsibilities. Inadequate segregation of duties increases the risk of errors being made and remaining undetected; it also may lead to fraud and the adoption of inappropriate working practices.

In any major IT System the following IT duties should be adequately segregated:

- System design and programming
- System support
- Routine IT operations and administration
- System security
- Database administration.

Physical Access control

Physical access controls include the environmental controls which operate across the whole IT environment and affect all underlying computer applications. These controls are designed to protect the computer hardware and software from damage, theft and unauthorised access. Access controls can operate on various levels, for example, from restricting access to the client's site, to installing key locks on individual PCs.

The IT Auditor should get a quick assessment of physical access controls. Restricting physical access to the IT systems reduces the risk of unauthorised persons altering the financial information.

Authorisation Control

Authorisation control helps verify the identity and authority of the person desiring to attempt a procedure or an operation. This control is exercised through use of passwords, signatures, smart cards, cryptographic systems etc. Such-controls ensure that only an authoriscd person has access to the system and its use, to enter and/or alter transactions, to take information etc.

Logical Access control

Logical Access controls are provided to protect the financial applications and underlying data files from unauthorised access, amendment or deletion. Logical access controls can exist at both an installation and application level. Controls within the general IT environment restrict access to the operating system, system resources and applications, whilst the application level controls restrict user activities within individual applications.

Logical access controls can also be used to restrict the use of powerful systems utilities, such as file editors. Logical access controls are often used with physical access controls to reduce the risk of the programs and data files being amended without authority. The importance of logical access controls is increased where physical access controls are less effective, for example, when computer systems make use of communication networks (LANs and WANs). The existence of adequate logical access security is particularly important where a client makes use of wide area networks and global facilities such as the Internet.

The most common form of logical access control is login identifiers (ids) followed by password authentication. For passwords to be effective there must be appropriate password policies and procedures, which are known to all staff and adhered to. Menu restrictions can be effective in controlling access to applications and system utilities.

Systems may be able to control access by identifying each individual user through their unique login ids and then having a pre-defined profile of authorised menus for each. The IT Auditor should consider how easy it would be for users to 'break out' of the menu system and gain unauthorised access to the operating system or other applications. Some computer systems may be able to control user access to applications and data files by using file permissions. These ensure that only those users with the appropriate access rights can read, write, delete or execute files.

Operation and file Controls

Operation and file controls are meant to ensure safeguarding the computer and computer files from unauthorised access, loss or theft. Controls relating to reception, conversion and processing of data and distribution of the final output promote the completeness and reliability of these operations and safeguard against the unauthorised processing of data or programmes. File controls and procedures adequately safeguard files and software against loss, misuse, theft, damage, unauthorised disclosure and accidental or deliberate corruption.

As the computer provides a means of holding, assessing and amending information, it is imperative that its use is controlled. There should be a definite schedule of work that is authorised to run on it and restrictions should be placed on the number and type of staff allowed access to it. Also, computer files are records of an organization which have to be well-safeguarded.

Change Management Controls

Change management controls are used to ensure that amendments to a computer system are properly authorised, tested, accepted and documented. Poor change controls could result in accidental or malicious changes to the software and data. Poorly designed changes could alter financial information and remove audit trails. Audit should ensure that a new or amended computer system is thoroughly tested by its end users before live use. Financial systems rarely remain static and are frequently changed, amended or updated. These regular changes may be necessary to improve efficiency, functionality or remove programming faults ('bugs').

IT Audit should emphasise that auditee organisations which update their computer systems should have appropriate change management and configuration management controls. Configuration management procedures relate to the control of IT assets (i.e. hardware, software, documentation and communications) and the subsequent update of records, whilst change management relates to the authorisation, impact assessment, asset update, testing and implementation of changes. Risks can be reduced by appropriate change management controls. These controls should ensure that all system and program amendments are satisfactorily justified, authorised, documented and tested and that an adequate audit trail of the changes is maintained. All change procedures should be documented

These controls should ensure that program and file amendments are authorised, logged and monitored. The ability to introduce new programs should be limited to authorised change control staff who are independent of computer programmers and staff who input transactions or maintain standing data.

Network Communication Security Controls

Network communication security controls are important where LANs/WANs or web enabled systems are in use. Some important aspects to be covered by this control are as follows:

(i) All sensitive information in the network should be protected by using appropriate techniques;

(ii) The critical network devices such as routers, switches and modems should be protected from physical damage;

(iii) The network configuration and inventories should be documented and maintained;

(iv) Prior authorisation of the Network Administrator should be obtained for making any changes to the network configuration.

(v) The changes made in the network configuration should be documented. The threat and risk assessment of the network after changes in the network configuration should be reviewed.

(vi) The network operation should be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

(vii) Physical access to communications and network sites should be controlled and restricted.

(viii) Communication and network systems should be controlled and restricted to authorised individuals.

(ix) Network diagnostic tools, e.g., spectrum analyzer protocol analyzer should be used on a need basis.

(x) Firewalls: Intelligent devices generally known as "Firewalls" should be used to isolate an organisation's data network from any external network. Firewall devices should also be used to limit network connectivity from unauthorised use. Networks that operate at varying security levels should be isolated from each other by appropriate firewalls. The internal network of the organisation should be physically and logically isolated from the

Internet and any other external connection by a firewall. All firewalls should be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter. All web servers for access by Internet users should be isolated from other data and host servers.

(xi) Connectivity: Organisations should establish procedures for allowing connectivity of their computer network or computer system to any outside computer system or networks. The permission to connect other networks and computer system should be approved by the Network Administrator and documented. All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines. The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network. As far as possible, no Internet access should be allowed to database server/file server or server hosting sensitive data. The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

(xii) Network Administrator: Each organisation should designate a properly trained "Network Administrator" who is responsible for operation, monitoring security and functioning of the network. Appropriate follow up of any unusual activity or pattern of access on the computer network should be investigated promptly by the Network Administrator. The system must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorised access, virus infection and hacking. Secure Network Management Systems should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized. Only authorised and legal software should be used on the network.

Business continuity Planning

The auditor should ensure that there are adequate plans to resume processing in the event of failure of computer operations. The degree of continuity planning will depend on the size of the IT department and the dependence on computer processing. A significant and prolonged loss of IT capability in a mission critical system may increase the risk of the financial statements being unavailable or materially mis-stated. Disaster recovery planning for IT facilities should be treated as one element of an organisation’s overall business continuity plan.

The extent of disaster recovery planning and the detailed measures required will vary considerably. Organisations with large IT departments, with mainframe computers and complex communication networks may require comprehensive, up to date recovery plans which incorporate standby facilities at alternative sites.

Disaster recovery plans should be documented, periodically tested and updated as necessary. Untested plans may be satisfactory on paper but fail when put into practice.

Testing will reveal deficiencies and allow amendments to be made. The importance of adequate documentation is increased where significant reliance is placed on a few key members of the IT department. The loss of key staff, perhaps due to the same reason the computers were disrupted, may adversely affect an organisation’s ability to resume operations within a reasonable timeframe.

Back-up copies of systems software, financial applications and underlying data files should be taken regularly. Back-ups should be cycled through a number of generations by, for example, using daily, weekly, monthly and quarterly tapes. Back-ups should be stored, together with a copy of the disaster recovery plan and systems documentation, in an off-site fire-safe. Where micro-computers are used, in addition to mini or mainframe computers, the auditor should ensure that there are also procedures for the backing-up of financial data stored on local hard disks.

Important points to be checked in general controls

The following points should be covered while reviewing these controls:

(i) obtain a list of hardware including, computer, ancillary and terminal equipment in use indicating model, performance details and check the existence of this equipment :

(ii) obtain an organisational chart which is up-to-date and see how the computer fits into the overall Organisation;

(iii) obtain an uptodate staff organization chart of the computer department showing the relative responsibilities and authorities and note any changes on review;

(iv) obtain job specification (role definition) for senior computer staff and supervisors of the ancillary section and note any changes;

(v) obtain the details of standards and norms fixed for each of the functions like data control, data preparation, system operation and verify their implementation :

(a) computer utilisation per shift in terms of CPU (Central Processing Unit) and peripheral use;

(b) key depressions per shift per data entry operator and error allowance;

(c) document standards and controls -batching, balancing and sequencing,

(d) run to run controls maintained by system operators;

(e) whether manuals are maintained and kept up-to-date specifying the control procedures and whether they are enforced in practice through a 'test check'.

(vi) obtain and verify, existence of the following terminal controls to protect data and system integrity

(a) physical access controls to terminal rooms;

(b) software controls through password protection and user directories;

(c) logging of terminal activities by all users.

(vii) obtain details of security measures, both physical and system, for check and review of the following :

(a) adequacy of protection of hardware and software against risk of fire (fire prevention steps and fire fighting arrangements) :

(b) maintenance of hardware and system software;

(c) air conditioning and protection against possible radiations, vibrations;

(d) possible industrial action, malicious action by programmers, operators, input-output staff (discontent among computer operating staff);

(e) security awareness and training provided to all employees;

(f) emergency shut-down procedures in case of power failures;

(g) safe custody of software and data files and type library;

(h) adequacy of back-up files (offsite storage included);

(i) operator access to program files and data;

(j) procedures for reconstructing files in the event of loss or disk errors/tape errors (contingency plans);

(k) computer equipment back-up through the use of compatible equipment at other dispersed sites;

(l) computer room should be off limits to all except systems operators, hardware engineers and

(m) insurance of the installation to cover possible risk.

Audit of Operation and Maintenance - 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.

Before getting on to evaluation of application controls, it will be necessary for an auditor to secure a reasonable understanding of the system. For this purpose, a brief description of the application should be prepared;

(i) indicating the major transactions,

(ii) describing the transaction flow and main output,

(iii) indicating the major files maintained and

(iv) providing approximate figures for transaction volumes.

Application Control requirements may be divided into:

(i) Documentation standards

(ii) Input control

(iii) Processing control

(iv) Output control

(v) Master/Standing Data File control

(vi) Audit requirements

Documentation Standards

Documentation standards ensure that adequate and up-to-date system documentation is maintained. Careful updating of documentation is also important. (Auditor will find documentation helpful as an aid to understanding the system but must be careful to ensure that it is up-to-date before using it.) There should be standards in auditee organisation to ensure that:

(i) system documentation is sufficiently comprehensive.

(ii) documentation is updated to reflect system amendments and

(iii) a back-up copy of the documentation is held.

Without good documentation, it will be difficult to assure that controls will operate on continuous basis and there will also be greater likelihood of error. Good application documentation reduces the risk of users making mistakes or exceeding their authorities. A review of comprehensive, up to date documentation should aid the auditor in gaining an understanding of how each application operates, and may help identify particular audit risks.

Documentation should include:

- a system overview;
- user requirements specification;
- program descriptions and listings;
- input/output descriptions;
- file contents descriptions;
- user manuals; and
- desk instructions.

Input Controls

The objective of Input control is to ensure that the procedures and controls reasonably guarantee that (i) the data received for processing are genuine, complete, not previously processed, accurate and properly authorized and (ii) data are entered accurately and without duplication. Input control is extremely important as the most important source of error or fraud in computerised systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

The controls that the auditor should evaluate are:

(i) all prime input, including changes to standing data, is appropriately authorised.

(ii) for on-line systems, the ability to enter data from a terminal is adequately restricted and controlled.

(iii) there is a method to prevent and detect duplicate processing of a source document,

(iv) all authorised input has been submitted or, in an on-line system transmitted and

(v) there are procedures for ensuring correction and resubmission of rejected data.

The controls outlined above may be invalidated if it is possible to by-pass them by entering or altering data from outside the application. There should be automatic application integrity checks which would detect and report on any external changes to data, for example, unauthorised changes made by personnel in computer operations, on the underlying transaction database. The results of the installation review should be reviewed to ensure that the use of system amendment facilities, such as editors, is properly controlled.

Data Transmission Controls

These controls are built in to IT Applications to ensure that data transmitted over local or wide area networks is valid, accurate and complete. Organisations using networks should ensure that there are adequate controls to reduce, to an acceptable level, the risk of data loss, unauthorised transactions being added and data corruption. Some computer systems are connected to either local or wide area networks (LANs or WANs), which allow them to receive and send data from remote locations. The more common data transmission media include telephone wires, coaxial cables, infra-red beams, optical fibres and radio waves.

Applications which transmit information across networks may be subject to the following risks:

- data may be intercepted and altered either during transmission or during storage at intermediate sites;
- unauthorised data may be introduced into the transaction stream using the communication connections; and
- data may be corrupted during transmission.

The integrity of transmitted data may be compromised through communication faults. The auditor should ensure that there are adequate controls in place, either within the network system, or the financial applications, to detect corrupted data. The network's communication protocol, i.e. the predetermined rules that determine the format and meaning of transmitted data, may incorporate automatic error detection and correction facilities. It is fairly easy to intercept transmitted data on most local and wide area networks. Inadequate network protection increases the risk of unauthorised data amendment, deletion and duplication. There are a number of controls that may be used to address these problems:

- Digital signatures may be used to verify that the transaction contents are intact and that the transaction originated from an authorised user;
- Data encryption techniques may be used to prevent the interception and alteration of transactions.

Processing Controls

Processing controls ensure complete and accurate processing of input and generated data. This objective is achieved by providing controls for:

(i) adequately validating input and generated data,

(ii) processing correct files ,

(iii) detecting and rejecting errors during processing and referring them back to the originators for re-processing,

(iv) proper transfer of data from one processing stage to another, and

(v) checking control totals (established prior to processing) during or after processing.

The objectives for processing controls are to ensure that:

- transactions processing is accurate;
- transactions processing is complete;
- transactions are unique (i.e. no duplicates);
- all transactions are valid; and
- the computer processes are auditable.

Processing controls within a computer application should ensure that only valid data and program files are used, that processing is complete and accurate and that processed data has been written to the correct files. Assurance that processing has been accurate and complete may be gained from performing a reconciliation of totals derived from input transactions to changes in data files maintained by the process. The auditor should ensure that there are controls to detect the incomplete or inaccurate processing of input data.

Application processes may perform further validation of transactions by checking data for duplication and consistency with other information held by other parts of the system. The process should check the integrity of data which it maintains , for example, by using check sums derived from the data. The aim of such controls is to detect external amendments to data due to system failure or use of system amendment facilities such as editors.

Computerised financial systems should maintain a log of the transactions processed. The transaction log, which may be referred to as the audit trail file, should contain sufficient information to identify the source of each transaction. In batch processing environments, errors detected during processing should be brought to the attention of users. Rejected batches should be logged and referred back to the originator. On-line systems should incorporate controls to monitor and report on unprocessed or uncleared transactions (such as part paid invoices). There should be procedures which allow to identify and review all uncleared transactions beyond a certain age.

Output Controls

These controls are incorporated to ensure that computer output is complete, accurate and correctly distributed. It may be noted that weakness in processing may sometimes be compensated by strong controls over output. A well-controlled system for input and processing is likely to be completely undermined if output is uncontrolled. Reconciliation carried out at the end of the output stage can provide very considerable assurance over the completeness and accuracy of earlier stages in the complete cycle.

Output controls ensure that all output is:

(i) produced and distributed on time,

(ii) fully reconciled with pre input control parameters,

(iii) physically controlled at all items, depending on the confidentiality of the document and

(iv) errors and exceptions are properly investigated and acted upon.

The completeness and integrity of output reports depends on restricting the ability to amend outputs and incorporating completeness checks such as page numbers and check sums.

Computer output should be regular and scheduled. Users are more likely to detect missing output if they expect to receive it on a regular basis. This can still be achieved where the subject of computer reports is erratic, such as exception reporting, by the production of nil reports.

Output files should be protected to reduce the risk of unauthorised amendment. Possible motivations for amending computer output include covering up unauthorised processing or manipulating undesirable financial results. Unprotected output files within a bill paying system could be exploited by altering cheque or payable order amounts and payee details. A combination of physical and logical controls may be used to protect the integrity of computer output.

Output from one IT system may form the input to another system, before finally being reflected in the financial statements, for example, the output from a feeder system such as payroll would be transferred, as input, to the general ledger. Where this is the case the auditor should look for controls to ensure that outputs are accurately transferred from one processing stage to the next. A further example would be where the output from a trial balance is used as the input to a word-processing or spreadsheet package, which then reformats the data to produce the financial statements.

Master/Standing Data File Controls

Master/Standing Data File controls are meant for integrity and accuracy of Master Files and Standing Data. Accuracy of data on Master and Standing files is of vital importance, to the auditor. Information stored in master and standing data files is usually critical to the processing and reporting of financial data. Information on master files can affect many related financial transactions and so must be adequately protected.These have to ensure that:

(i) amendments to standing data are properly authorised and controlled.

(ii) integrity of Master and Standing Files is verified by checking, control totals and periodic reconciliation with independently held records.

(iii) special amended facilities are properly recorded in and then use controlled by management authorisation and subsequent review and

(iv) physical and logical access to application data files are restricted and controlled.

Audit Requirements

Audit requirements have to be provided to ensure that the system can be audited in an effective and efficient manner. Audit trail has to be maintained to enable tracing of an item from input through to its final destination and break up a result into its constituent parts. (Auditors may have to use audit software or test data for the efficient execution of their audit. They have, therefore, to seek reasonable requests for the access to copies of system data files, report generators and processing time).

Before considering the audit requirements for a system being developed, the auditor should have a knowledge of the currently existing system and should keep in mind:

(i) weakness in the current system affecting the audit approach,

(ii) features in the existing system, which are relied on to provide an effective audit, that should be retained in the new system, and

(iii) additional facilities, not currently provided which would assist the audit of the new system.

Important points to be checked in application controls

Audit of an application system which is operational involves verification of input/output controls, processing controls and audit trail. Evidence may be obtained on the following points in the course of audit to come to a reasonable conclusion regarding existence of controls and their adequacy:

(i) Whether the data processed are genuine, complete, accurate and not provisional?

(ii) Whether expected output is produced and distributed on time?

(iii) Whether application programs process the data as intended and accurately?

(iv) Whether a complete audit trail is available for tracing back a transaction from the final result to the initial input?

(v) Whether the data and changes to it are authorised by appropriate authority both in the user and computer departments?

(vi) Whether schedules for receipt of input data are maintained and what is the extent of compliance?

(vii) Whether there is a preliminary check on input data to ensure completeness?

(viii) Whether the application system provides for the following programmed controls:

(a) Check for missing/duplicate transactions: Examples are (i) check for continuity of goods invoice numbers issued by a station for missing numbers (ii) more than one subscription for the same month for one PF account number

(b) Controls on rejected items and keeping them under computer suspense: Examples are (i) the monthly treasury transactions are rejected if they do not have valid heads of account as given in the budget master. The rejected items are kept under suspense and control totals along with valid transactions tallied with the cash account and list of payments (ii) Rejection of issue notes in a stores accounting system due to want of balances.

(c) Input validation for data purification (alpha- numeric checks to conform to data types): Examples are (i) Personal identity number should be numeric (ii) Station name field is alphabetic (depends on system requirements)

(d) Limit/range checks: Examples are (i) the transaction type in a financial accounting system (expressed in terms of rupees), should not have values less than 1 or greater than 6 (ii) The maximum basic pay cannot exceed Rs. 9000/- per month (iii) The code for treasury alone for any State should have values not exceeding two digits.

(e) Overflow checks: Examples are (i) if the field length for withdrawal/advances in a PF system is 5 digits and there is a valid debit transaction with 6 digits, the high order digit gets truncated, i.e., the debit will be recorded by one digit less (ii) In arithmetic operations like weight multiplied by rate to give freight, if adequate field length is not provided for 'freight' the transaction will be incorrectly recorded as it will be confined to the field length.

(f) Some fields should not be blanks or zeros (mandatory fields): Examples are (i) in a leave accounting system, the leave type code cannot be left blank since the entire transaction will be invalid without this (ii) a treasury transaction should indicate in the relevant fields whether it is voted/charged, plan/non-plan, and not be left blank.

(g) Check digits: Examples are (i) in a pay roll system, the account number, which is a control field to identify an employee, has a built-in check digit. The program works out the check digit on the basis of the account number input and verifies the correctness of check digit given. If the check digits do not tally, then the account number is wrongly entered (may be a transposition error). (ii) the station code in the freight accounting system in the Railways has a check digit to detect data entry errors this code.

(h) Compatibility checks: Example is if the transaction type is for official receipts in a financial accounting system, the amount cannot normally be a negative value.

(i) Exception condition check: Example is the amount column in a treasury transaction for a month has a value greater than the budget for a quarter.

(j) Total for a batch/lot: for example the batch total for a major head under a treasury is worked out on the computer and tallied with the total given in the schedule of payments/receipts for that batch (to ensure complete accounting of transactions in a batch)

(k) Record totals and summaries for reconciliation: Example is in a freight accounting system, when a goods basic tape is created it gives the total number of records, which should tally with the total number of invoices input.

(ix) Whether output reports are test-checked before, being distributed to the user department and the output is produced in accordance with a prescribed schedule.

Audit Trail

Objective of audit trail is to obtain sufficient evidence matter regarding the reliability and integrity of the application system. To achieve this, the audit trail should contain enough information to allow management, the auditor and the user:

(i) to recreate processing action;

(ii) to verify summary totals and

(iii) to trace the sources of intentional and unintentional errors.

The audit trail should include the following information:

- System information including start up time, stop time, restarts, recovery etc.
- Transaction information including input items which change the database, control totals and rejected items (relevant to database applications).
- Communication information including terminal log-on/off, password use, security violation, network changes and transmission statistics (relevant to transaction processing i.e. TP applications).

In a computer system, the audit trail may not always be apparent as in a manual system since data are often retained in magnetic media and output is limited to a small number of total items processed, with reports produced only on exception basis. The general procedure is to first investigate control totals and run to run totals within the whole system and then to check and substantiate the audit trail by limited checking through records and files or by taking intermediate printouts of audit interest. If the design of the computer system does not provide for adequate audit trail this should be brought out in audit review, highlighting control weaknesses or lack of controls in the system. Apart from errors that might creep into the system, there is a possibility of frauds, which might occur due to undetected control weaknesses.