ASOSAI

6th ASOSAI Research Project

IT Audit Guidelines

Research Team Members:

Malaysia
India
Australia
China

September 2003

TABLE OF CONTENT

LIST OF APPENDICES

Foreward

The 6th ASOSAI Research Project on Audit of IT was approved by the 31st ASOSAI Governing Board Meeting held in October 2002 in Manila. Four SAIs were appointed as members of the research team, namely Australia, China, India and Malaysia with Malaysia as the team leader.

The research team met three times over the period April to August 2003 to plan for the implementation; discuss on the research progress; as well as prepare for the final draft in the form of 'IT Audit Guidelines'. The research project was successfully completed within a period of six months and this achievement was made possible through our constant discussions via the e-mail and of course with full co-operation of team members.

During our first meeting in May 2003 held in Kuala Lumpur, the IT Audit Manual of the National Audit Department, Malaysia was used as reference in the formulation of the research framework aided by supplementary materials on IT Audit from sources such as the INTOSAI/ASOSAI Training Materials, ISACA, CoBIT and others. The guidelines have taken into account the International and INTOSAI Auditing Standard relevant to IT Audit and the content comprises of basic requirements and audit procedures in the performance of IT Audit. The team in drafting the guidelines has also taken into account the varying degree of IT Audit work undertaken by the ASOSAI members. To avoid ambiguity and confusion to newcomers to IT Audit, the guidelines was drafted with simplicity and conciseness. Furthermore, it is our belief that the practical details of IT Audit are best delivered through the ASOSAI Training Programme where the theoretical understanding on IT Audit will be reinforced through the hands-on training.

Similar to the other guidelines issued by the ASOSAI, these guidelines are also 'living document'. Continuous efforts should be made to update its contents to keep in pace with the technological and environmental change to maintain its relevancy and acceptability among ASOSAI members as an authoritative document on IT audit.

For the implementation of this research project, each SAI was assigned to prepare the initial draft based on the consensus reached during the Kuala Lumpur meeting. The drafts on the respective parts were circulated among members for their perusal and were discussed in subsequent meetings. In mid August 2003, the first draft was circulated to all ASOSAI members for their comments. During our final meeting held in Canberra from the 25th to 26th of August 2003, we decided to re-distribute the final draft which had taken into account comments and suggestions made by team members during that meeting. ASOSAI members were given the opportunity to give their comments until the 22nd September 2003 before the final document is submitted to the Secretary-General of the ASOSAI for consideration to be tabled during the 9th ASOSAI Assembly in Manila.

The guidelines comprise of four parts, Part I on IT Framework, Part II on IT Control Audit, Part II on Information System Audit, and Part IV on Computer Assisted Audit Techniques and Tools (CAATTs). The guidelines introduce auditors to IT Audit Framework where aspects on IT environment and controls; established IT Audit Standards; related audit risks; and types of IT audit that could be performed as an integral part of the traditional audit are explained. These guidelines also highlight some salient features of control assessment frameworks, samples on survey questionnaires on preliminary assessment of IT environment and primary features of IT controls, sample on work programme for audit of system development and illustrations on the use of CAATTs. Based on our research from the established sources on IT Audit, we believed the scope of the guidelines has sufficiently covered the basic requirements for conducting an IT Audit, and strongly recommend that ASOSAI members utilise them as the 'Best Practices Guide on IT Audit'.

The team members of this research comprised of Mr. Abdul Rashid Yaakub and Mr. Khalid Khan (Malaysia), Mr. P.K. Brahma and Mr. Rajesh Goel (India), Mr. Wayne Jones (Australia) and Mdm. Yang Li (China). The team would like to express its special gratitude to His Excellency Datuk Dr. Hadenan Abdul Jalil, Auditor-General of Malaysia who have strongly supported the project and provided the much needed leadership in ensuring the successful completion of this research project. He had taken the effort to lead the final discussion of the research team and contributed towards the finalisation of these Guidelines. The team would also like to express its thanks to ASOSAI fraternity for giving their comments on the draft and the ASOSAI Governing Board for giving the opportunity to carry out this research project.

Preamble

These guidelines aim to provide an established source of reference on IT Audit for the ASOSAI fraternity. It is by no means an exhaustive or definitive document of IT Audit. However, users of these guidelines are assured of the basic requirements in conducting on IT Audit in accordance with universally accepted practices in this area.

Part I of these guidelines set up the conceptual framework for thinking about IT Audit. It introduces reader on IT Environment and IT Controls; universal IT Audit Standards; risk issues, and the application of IT as an integral part of the overall audit process.

Part 2 of these guidelines present the General, Application and Specific Controls in an IT environment that IT Auditors need to identify, evaluate and finally formulate test procedures to assess these controls. More importantly in Part 2, salient features of several established control assessment frameworks are highlighted. For clarity, discussion on the various controls is structured as follows: controls objectives, risk areas and audit procedures. Sample Audit Programmes for evaluation of IT controls are appended for reference.

Part 3 introduces IT Auditors to approaches in Development Audit i.e. Ongoing Project Audit and Post Implementation Audit. The importance of both approaches to assist IT project implementation as well as risk areas are also discussed. Key features to ensure successful IT Project implementation are discussed under the following topics: Project Management, Risk Management, Finding, Deliverables and Adherence to Standard. System Development Life Cycle methodology of system development is discussed in greater detail for guidance. A sample Audit Programme for evaluating System Development is appended for reference.

Part 4 introduces IT Auditors to the capabilities, basic steps, types and categories of CAATTs. As a guide to auditors, two examples on the usage of CAATTs are illustrated. Part 4 also introduces some background on sampling.

PART 1 IT AUDIT FRAMEWORK

INTRODUCTION

1.1 The use of Information and Communication Technology (ICT) within government entities has become increasingly significant in recent years, particularly following greater use of the Internet and organisational intranets. Technology has increased the amount of data and information being processed and it has significantly impacted the control environment. ICT is also now a key component of government entities business strategies and core business processing activities. The management of ICT risk has therefore been elevated within entities and now forms a key part of corporate governance. Accordingly, the effective and efficient management of ICT is vital to the success of most entities.

1.2 As computer technology has advanced, Government organisations have become increasingly dependent on computerised information systems to carry out their business operations and service delivery and to process, maintain and report essential information. There are also an increasing range of ICT vulnerabilities and threats that have to be effectively and efficiently managed. As a consequence, the confidentiality, integrity, availability and 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 effectiveness and efficiency of IT controls in information systems and related operations to ensure they are operating as intended.

IT AUDIT

1.3 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'*.[1] 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 auditors 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.

1.4 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. The highly repetitive nature of many computer applications means that small errors may lead to large losses. For example, 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. This makes it imperative for the auditor to test the invisible processes and to identify the vulnerabilities in a computer information system, as through errors and irregularities, the costs involved can be high.

1.5 Increasing use of computers for processing organisational data has added new scope to the review and evaluation of internal controls for audit purposes. The IT internal controls are of great value in any computerised system and it is an important

[1] Weber, R., Information Systems Control and Audit, 1999

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 internal controls should be commensurated with the risk assessed so as to reduce the impact of identified risks to acceptable levels. IT auditors need to evaluate the adequacy of internal controls in computer systems to mitigate the risk of loss due to errors, fraud and other acts and disasters or incidents that cause the system to be unavailable.

NEED FOR IT AUDIT

1.6 Management employing the use of information systems have objectives and expectations of what they intend to achieve from the large investment made in utilising technology. Reasons for implementing ICT within the organisation include the desire to obtain business value through reduced costs, greater effectiveness, enhanced efficiency and/or increased service delivery. It is against these objectives that an IT auditor is required to provide management assurance. Typically, management's goals and objectives in utilising technology to support business processes include:

- Confidentiality;
- Integrity;
- Availability;
- Reliability; and
- Compliance with legal and regulatory requirements.

Underpinning these goals and objectives is the need to ensure information technology, and the controls supporting such technology, assists the organisation to achieve its business objectives (effectiveness) with appropriate use of resources (efficiency).

Confidentiality

1.7 'Confidentiality concerns the protection of sensitive information from unauthorised disclosure.'[2] Consideration needs to be given to the level of sensitivity to the data, as this will determine how stringent controls over its access should be. Management need assurance of the organisation's ability to maintain information confidential, as compromises in confidentiality could lead to significant public reputation harm, particularly where the information relates to sensitive client data.

Integrity

1.8 Integrity refers to 'the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.'[3] This is an important audit objective to gain assurance on because it provides assurance to both management and external report users that the information produced by the organisation's information systems can be relied and trusted upon to make business decisions.

Availability

1.9 'Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary

[2] http://www.isaca.org/glossary.htm
[3] http://www.isaca.org/glossary.htm

resources and associated capabilities.'[4] Given the high-risk nature of keeping important information stored on computer systems, it is important that organisations gain assurance that the information they need for decision-making is available when required. This implies ensuring that the organisation has measures in place to ensure business continuity and ensuring that recovery can be made in a timely manner from disasters so that information is available to users as and when required.

Reliability

1.10 Reliability refers to the degree of consistency of a system or the ability of a system (or component) to perform its required function under stated conditions. Reliability is an important audit objective in order to provide assurance that the system consistently operates and performs its stated functions as expected.

Compliance with Legal and Regulatory Requirements

1.11 'Compliance deals with complying with those laws, regulations and contractual obligations to which the business process is subject, that is, externally imposed business criteria.'[5] Management and key stakeholders require assurance that necessary compliance procedures have been put in place, as there is a potential risk that the organisation could incur penalties should legal and regulatory procedures not be enforced.

IT AUDIT STANDARDS

1.12 There is wide recognition that the specialised nature of IT auditing and the skills necessary to perform such audits, require standards that apply specifically to IT auditing. In response to this need, various professional and government organisations develop and maintain standards and guidelines for IT auditing.

1.13 The professional standards provide a framework for all audits and auditors and define the mandatory requirements of the audit. They are a broad statement of auditors' responsibilities and ensure that auditors have the competence, integrity, objectivity and independence in planning, conducting and reporting on their work. The guidelines supporting the professional standards assist the auditor to apply the standards and provide examples that an IT Auditor might follow to meet these standards.

1.14 In addition to IT auditing standards, IT auditors need to be alert to other laws, regulations, or other authoritative sources that may impact upon the conduct of an IT audit. For example, national, state and local laws and regulations may have to be taken into consideration in planning and conducting IT audits.

1.15 When determining the scope of issues to be addressed in any review of computer related controls, IT auditors should consider issues of electronic data confidentiality, integrity, availability and reliability. The IT audit work carried out by SAIs should be guided by international standards or the respective national IT auditing standards. These may include INTOSAI Auditing Standards, International Federation of Accountants (IFAC) Auditing Standards, international standards of professional IT audit organisations, such as the Information System Audit and Control Association (ISACA) and the Institute of Internal Auditors (IIA) and national auditing

[4] http://www.isaca.org/glossary.htm

[5] Gelinas & Sutton, Accounting Information Systems, South-Western Thomson Learning,2002.

standards of SAI member countries. IT auditors should familiarise themselves with these standards before starting an IT audit.

1.16 Appendix 1.1 of these guidelines provides more details on a number of key IT auditing standards.

IT AUDIT OBJECTIVES

1.17 The objective of undertaking an IT audit is to evaluate an auditee's computerised information system (CIS) in order to ascertain whether the CIS produces timely, accurate, complete and reliable information outputs,[6] as well as ensuring confidentiality, integrity, availability and reliability of data and adherence to relevant legal and regulatory requirements. Audit objectives will vary according to the nature or category of audit i.e. a financial statement or performance audit. For example if the audit has a financial focus, then the primary objective will be to offer an opinion as to whether the financial statements reflect a true and fair view of the entity's financial position.

1.18 The objectives of undertaking an IT audit as a component of a financial statement audit include to:

- Understand how well management capitalises on the use of information technology to improve its important business processes;
- Understand the pervasive effect of information technology on the client's important business processes, including the development of the financial statements and the business risks related to these processes;
- Understand how the client's use of information technology for the processing, storage and communication of financial information affects the internal control systems and our consideration of inherent risk and control risk;
- Identify and understand the controls that management uses to measure, manage and control the information technology processes; and
- Conclude on the effectiveness of controls over the information technology processes that have a direct and important impact on the processing of financial information.[7]

1.19 Where IT audit is involved in the performance audit, the objectives of the audit are further defined by what role IT is playing in the audit.

- If the performance audit has an IT focus, the objective will be to seek assurance that all aspects of the IT systems, including necessary controls, are being effectively enforced.
- The performance audit could alternatively be examining the efficiency and effectiveness of a business process/government program and as such IT audit is involved because IT is considered critical in the organization being able to deliver those services. As such, the focus of the IT audit is to provide assurance that the IT systems can be relied upon to help deliver those services. The efficiency and effectiveness of those services are then examined from a non-IT perspective after considering the impact that IT has on the ability of the organization to deliver those services.

[6] The National Audit Department of Malaysia, ICT Audit Guideline 2001

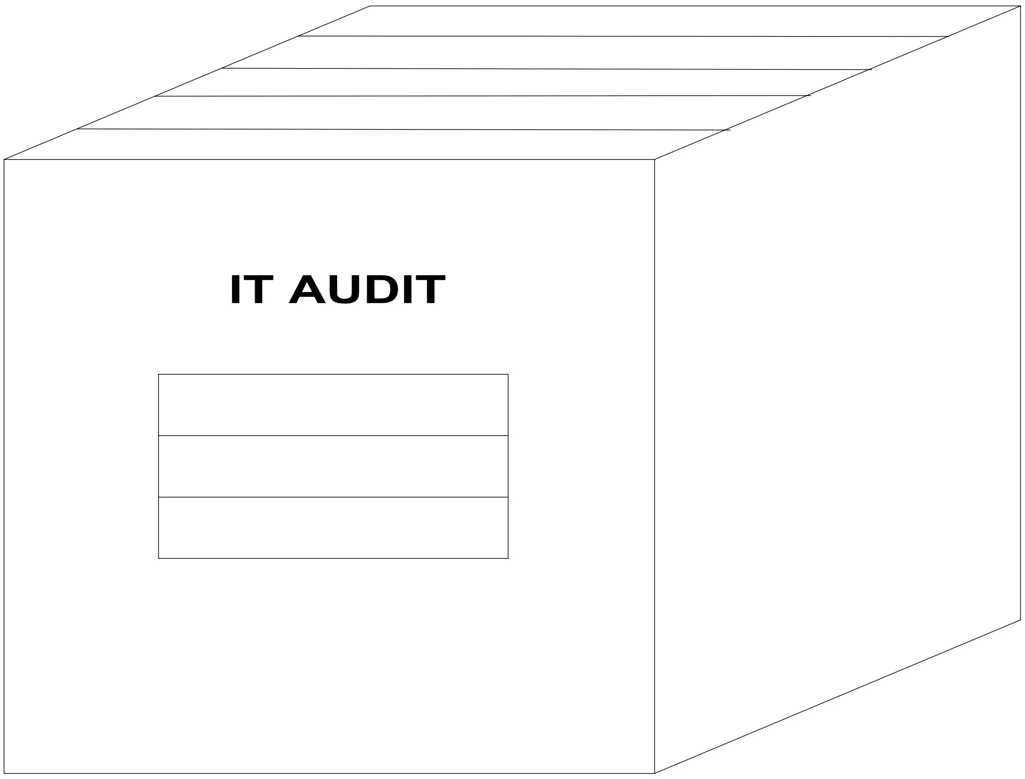
[7] EY Audit Methodology, Activity 8

IT ENVIRONMENT

1.20 It is necessary for the auditor to obtain a clear understanding of the IT environment in which the CIS operate to be able to provide adequate assurance on these objectives. This will ultimately determine the nature and scope of the audit to be undertaken and will also ensure that the auditor has focused their work in the appropriate areas so that the auditor has an appropriate basis upon which to make final assessment of the IT environment.

1.21 Given the complexity involved in large information systems and the monumental task of examining and evaluating all data processing, it is appropriate to examine the CIS from different viewpoints, thus narrowing the scope of the audit and allowing the auditor to concentrate on those aspects of the system that pose the greatest risk to compromising management's goals and objectives from employing those information systems. The diagram below graphically depicts the entire IT audit environment and the interaction between the different elements.

IT AUDIT ENVIRONMENT



IT CONTROLS

1.22 IT controls involve an entity's board of directors, management and other top personnel and are designed to provide reasonable assurance regarding the achievement of objectives in the categories:

- Effectiveness and efficiency of operations

- Reliability of financial reporting
- Compliance with applicable laws and regulations

1.23 IT controls in a CIS include the entire manual and programmed methods, policies and procedures that ensure the protection of the entity's assets, the accuracy and reliability of its records and the operational adherence to the management standards.

1.24 The ASOSAI IT Audit methodology uses a top-down, risk-oriented approach in the evaluation of controls. The following steps provide an overview of the tasks involved in review of IT controls:

Phase	Description
Planning	This phase facilitates the IT auditor in gaining an understanding of the agency, its organisational structure and operations. The IT auditor obtains an understanding of the entity's computer related operations and controls and related risks in view of inherent IT risks. From this understanding the auditor evaluates the overall IT control environment and makes a preliminary risk assessment. The results of the assessment will guide the extent of procedures to be employed in subsequent phases of the audit.
Verification and Testing	During this phase of auditing, IT auditors obtain detailed information on control policies, procedures and objectives and perform tests of control activities. The objectives of these tests are to determine if controls are operating effectively. General controls as well as application controls must be effective to help ensure the confidentiality, integrity, availability and reliability of critical computer processed data.
Reporting Phase	During the reporting phase, the IT auditor draws conclusions and develops a report in order to communicate the objectives of the audit, the audit scope, the methodology adopted and the findings, conclusions and recommendations.

1.25 In CIS environment, the control components found in manual systems must still exist. However, the use of computers affects the implementation of these components in several ways. IT controls are used to mitigate the risks associated within the IT environment and application systems and are broadly classified into three categories. These controls are part of the overall internal control process within any auditee's organisation:

- General Controls
- Application Controls
- Specific Controls

General Controls

1.26 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, business continuity planning, IT project management, etc.

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

- Organisation and Management (IT policies and standards);
- IT Operation Controls;
- Physical Controls (access and environment);
- Logical Access Controls;
- Acquisition and Programme Change Controls; and
- Business Continuity and Disaster Recovery Controls.

Application Controls

1.28 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 inputs, 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.

1.29 Application controls are unique 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, complete, authorised and recorded.

1.30 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 an auditee's accounts. It would not be obvious that testing the auditee's general IT controls (e.g. change control procedures) would provide a similar level of assurance for the same account balance.

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

- Controls over the input of transactions;
- Controls over processing;
- Controls over output; and
- Controls over standing data and master files.

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

Specific Controls

1.33 Specific control issues that cover the following:

- Network and Internet controls including the risk associated with networks and internet controls.
- End user computing controls including risks associated with end user computing and the associated controls.
- e-Governance
- IT Security Policy
- Outsourcing Policy

APPLICATION OF IT AUDIT

1.34 An IT audit is part of the overall audit process. Therefore, it is important to have an understanding of the various types of IT audits that can be conducted. This understanding is required so that the development of audit programs and procedures is appropriately focused and their execution will ultimately satisfy the specific audit objectives. In short this means collecting and analysing evidence in an IT environment in order to conclude against pre-defined audit objectives.

1.35 IT audit can be applied in the implementation of Financial Audits, Performance Audits and Information System Development Audits.

Financial Audit

Introduction

1.36 The purpose of a financial audit is to express an opinion on the financial statements and financial accountability of public sector entities. The overall purpose of the IT component of a financial audit is to asses the reliability of IT controls that support the processing of financial records. This includes assessing the effectiveness and efficiency of IT controls through evaluating the IT environment to understand how well management uses technology and how pervasive IT is on important business processes.

Planning

1.37 In undertaking an IT audit as a component of a financial audit, the audit approach should be risk based. There are four procedures that should be planned for in developing the approach in order to be able to conclude on the effectiveness of controls over the information technology processes that have a direct impact on the processing of financial information:

- Determine the scope of our analysis of the information technology processes by identifying how they support important business processes and the processing of financial information;
- Obtain background information about the auditee's IT environment, including information about and applications supporting the critical business processes, together with the underlying platforms and those to which they are networked;

- Conduct a walk-through of those information technology processes deemed to have a direct and important effect on the processing of financial information to confirm our understanding of the process design and related controls;[8] and
- Based upon our understanding of the information technology processes, evaluate the effectiveness of the design of each of the major information technology processes and related internal controls. If an evaluation cannot be made at the major process level, understand the information technology process at a lower level (e.g. sub-process level) and evaluate the effectiveness of the design of the sub-process. For those information technology processes that do not have a direct and important effect on the processing of financial information, we make a business decision regarding the additional work, if any, to be performed.

Reporting

1.38 The obligation for financial statement reporting will largely be dependent upon the individual requirements of each SAI in accordance with the applicable standards and regulations of the country.

1.39 While individual practices vary between SAI's, the most common form of audit reports will be:

Report	Purpose
Management Letters	Report to management of audited agency for comment and feedback. Details internal control issues with implications and recommendations.
Draft Audit Report	Report to management of audited agency for confirmation. Summarizes audit control issues and identified management opportunities for improvement.
Final Audit Report	Report to the highest authority e.g. Parliament, King, President, etc. as directed in the respective SAI's mandate. Summarizes major findings and implications followed by individual agency issues

Audit Risks

1.40 The IT Auditor, in undertaking an IT audit as a component of a financial audit needs to be aware of a number of risks that organisations face. In taking a risk-based approach, the auditor can focus on those areas that pose the greatest risk to the organization not presenting fair and true financial statements.

1.41 The IT auditor should be aware of the following common areas that present potential risks in a computing environment that are relied upon to produce financial data:

- The auditee develops and operates their own applications rather than outsourcing and the use of established industry and financial packages;
- Aspects of the entity's industry or internal environment may affect the development and application of controls. For example competitive pressure to introduce Electronic Data Interchange may result in the entity using a CIS that is not adequately controlled or performing in accordance with specifications;

[8] EY Audit Methodology, Activity 8

- The users have or can grant access to specific functions or data;
- Users have the ability to change data and develop reports (for example to change data or formulae on spreadsheets);
- Pervasive CIS controls (such as systems development and program maintenance and control over users' access to sensitive functions) affect the reliability of all application systems that are processed on the computer. The impact of these controls is dependent on both the extent to which they apply to specific applications (for example whether the aspects of the systems in which the auditor has an interest are developed and controlled centrally) and the extent to which the quality of the controls is appropriate to the level of risk associated with that application (or the aspect of the application in which the auditor has an interest);
- The nature and extent of documentation regarding the CIS is appropriate given the complexity of and inherent risks faced by the CIS environment;
- Factors that affect the quality of audit evidence available, for example a paperless environment, may increase the potential for audit evidence to be incomplete, unreliable or difficult to obtain;
- Specific risks associated with a particular CIS environment are identified, for example electronic funds transfer systems where the risk of irregularities may be increased or a complex CIS environment where the risk of error may be higher;
- End-user computing, which refers to any individual exercising control over and using a particular resource or more particularly a software application, is used to produce financial information, in particular where this use may be more susceptible to manipulation; and
- Users lack the time, discipline or knowledge to effectively monitor the results of processing.[9]

Performance Audits

Introduction

1.42 The purpose of a performance audit is to evaluate the efficiency, economy and/or administrative effectiveness of public sector entities. Performance auditing promotes public accountability and is an aid to good corporate governance.

1.43 IT auditing can play one of two roles in the performance audit. One role concerns where IT is the main focus of the audit. Therefore, the audit's objectives include examining an organisation's IT systems and how the organisation is performing against benchmark performance. Secondly, an IT audit as a component of a performance audit can seek to support the work of a performance audit that is focused on the efficiency and effectiveness of business processes/government programs. IT will play an important role in such audits, as IT systems will typically be relied upon to help deliver the services that are under examination during the audit and therefore the IT auditor will be required to assess the impact of IT on processes and government programmes and activities.

[9] Extracted from CPA Australia Members' Handbook December 2002 issue, AUS214 Auditing in a CIS Environment.

Objectives

1.44 Generally, performance auditing has the objective of improving public sector administration and assurance about the quality of management of public resources. Performance auditing may therefore lead to better accountability, improved economy and efficiency in the acquisition of resources, improved effectiveness in achieving public sector program objectives, a higher quality in public sector service delivery and improved management planning and control. [10]

Planning

1.45 Audit topics are generally selected on two grounds: firstly, to focus on audits expected to add maximum value in terms of improved accountability, economy, efficiency and effectiveness; secondly, to ensure appropriate coverage of program operations within the limitations of audit resources available.[11]

1.46 The analysis of risks of poor performance or, expressed another way, risks of inadequate economy, efficiency and effectiveness will lead to a list of potential audit topics. It can be useful to rank the topics subjectively against the following criteria:

- Overall estimated audit impact;
- Financial materiality;
- Risk to good management;
- Significance of the program to the activities of the agency;
- Visibility of the program/activity as reflected in its political sensitivity
- and national importance; and
- Lack of recent audit coverage and other internal and external review of the program/activity.[12]

1.47 Following selection of the audit topic, the audit needs to be planned effectively to ensure the objectives of the audit are achieved. Therefore, the IT auditor needs to take into account the following important aspects of audit planning:

- Have or obtain a knowledge of the business sufficient to enable the auditor to identify and understand the events, transactions and practices that, in the auditor's judgment, may have a significant effect on the performance information or on the audit or audit report;
- Establish or assess the audit objectives;
- Establish or assess the audit scope;
- Identify suitable criteria to enable the auditor to assess the matters subject to audit;
- Develop and document an audit plan describing the expected scope and conduct of the audit and an audit program setting out the nature, timing and extent of planned audit procedures required to implement the audit plan;

[10] Fifth ASOSAI Research Project: Performance Auditing Guidelines, ASOSAI, October 2000

[11] Fifth ASOSAI Research Project: Performance Auditing Guidelines, ASOSAI, October 2000

[12] Fifth ASOSAI Research Project: Performance Auditing Guidelines, ASOSAI, October 2000

- Assess whether the audit staff have adequate skills, competence and knowledge to undertake the audit and where knowledge of a specialised area is essential, whether it is appropriate to engage an expert or include specialists as part of the audit team.[13]

Reporting

1.48 Performance audit reports should be timely and objective, with issues firmly expressed having regard to the circumstances. Where dealing with significant issues, there should be a logical and compelling exposition of the issue and exposures. To maximise the effect of the report on improving public administration, care must be taken to ensure it is accurate, complete, defensible, understandable and balanced.

1.49 Significant issues and recommendations should be highlighted in a summary of the report. The auditor should review and assess the conclusions drawn from the audit evidence obtained as the basis for preparing the audit report.

1.50 Performance audit reports vary according to the differences in audit mandates and the scope and complexity of the particular audit and its findings. The performance audit mandate, whether established by legislation, by directive from the governing body or by contract, ordinarily specifies the minimum audit and reporting requirements of the performance audit.[14]

1.51 Where the IT audit is a component of a performance audit, the auditor may be required to produce an internal report to the performance audit team on how the performance audit team can rely on the IT systems for the remaining aspects of the audit. Furthermore, the IT auditor, whilst in this case will not produce the final audit report, may be responsible for an aspect of the report and as such will need to liaise with the performance audit team.

Audit Risks

1.52 The major risk when undertaking a performance audit centres on the robustness of the planning process. The auditor must obtain a comprehensive understanding of the program or area to be audited to ensure the audit is conducted in an efficient and effective manner. The auditor must also establish relevant audit criteria in order to enable the auditor to assess of the matters subject to audit.

1.53 Understanding an audit entity is not a discrete part of the audit process. Rather it is a continuous process. Typically, the auditor will commence with a broad understanding of the program subject to audit and will develop and enhance this understanding during detailed audit planning, the conduct of any preliminary studies and execution of fieldwork.

1.54 When planning the audit, audit criteria should be established as the reasonable and attainable standards of performance against which the audit activities can be assessed. In order to ensure that appropriate conclusions are drawn about the entity's operations, criteria must be relevant to the matters being audited and appropriate to the circumstances. Therefore, it is crucial that audit criteria are discussed and where appropriate, agreed with the auditee before the start of the audit. This is to avoid audit findings being challenged as 'out of scope' at the end of the audit. Audit criteria reflect the desirable control model for the subject under review and they represent

[13] Australian Auditing Standard AUS 808: Planning Performance Audits

[14] Fifth ASOSAI Research Project: Performance Auditing Guidelines, ASOSAI, October 2000

good practice – an expectation of 'what should be'. Incorrectly specified audit criteria could cause the audit to generate incorrect audit findings.

Information System Development Audit

1.55 Information system development audit ensure control over the entire development process from the initial idea or proposal to acceptance of a fully operational system are complied satisfactorily.

1.56 While the IT Auditor may not be an IT developer, programmer or technician, the auditor's overall contribution generally is to ensure:

- Controls are identified and developed into the new system;
- Controls exist to manage the project and development project decisions are transparent;
- Predetermined standards are set (and followed);
- Development specifications make sense and are cost effective;
- That future technology improvements are considered;
- Systems are robust and reliable, secure from unwanted interference and auditable; and
- The development objectives are clear and achievable.

1.57 Efficiency of systems is an important aspect of system capability that leads to effective use of resources. A key is controlling system development to prevent cost overruns and systems that do not perform as required.

1.58 **It is advisable that the auditor in performing IT audit understand the steps discuss in the following Parts of this manual.**

PART 2 IT CONTROL AUDIT

SCOPE

2.1 The purpose of the IT Control Audit module of these Guidelines is to provide guidance and procedures to IT Auditors for application in the areas of risks, controls and audit considerations related to Information Systems. It also assists IT Auditors in the scope of issues that generally should be considered in any review of computer related controls over the integrity, confidentiality and availability of electronic data. It is not an audit standard; however, the IT Control Audit work carried out by SAIs may be influenced by different International or National Auditing standards. The salient features of some of the well known control assessment frameworks have also been reproduced in Appendix 2.1.

DEFINITION OF IT CONTROLS

2.2 The capabilities of computer systems have advanced rapidly over the past several decades. In many organisations, the entire data has been computerised and all the information is available only in digital media. In this changed scenario, auditors have to adapt their methodology to changed circumstances. While the overall control objectives do not change in an IT environment, their implementation does. The approach of auditors to evaluate internal controls has to change accordingly.

2.3 IT Controls in a computer information system are all the manual and programmed methods, policies and procedures that ensure the protection of the entity's assets, the accuracy and reliability of its records and the operational adherence to the management standards[15].

CONTROLS IN A COMPUTERISED ENVIRONMENT

2.4 In an IT environment, the control components found in manual systems must still exist. However, the use of computers affects the implementation of these components in several ways. Information Technology controls are used to mitigate the risks associated with application systems and the IT environment and broadly classified into two categories.

2.5 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 third party service providers employing their own standards and controls, making these systems vulnerable to remote and unauthorised access.

2.6 IT Control Audit involves two types of testing – compliance and substantive testing. Compliance testing determines if controls are being applied in the manner described in the programme

documentation or as described by the auditee. In other words, a compliance test determines if controls are being applied in a manner that "complies with" management policies and procedures. Substantive audit "substantiates" the adequacy of existing controls in protecting the organisation from fraudulent activity and encompasses substantiating the reported results of processing transactions or

[15] ASOSAI IT Audit Training Courseware

activities. With the help of CAATTs software, IT Auditor can plan for 100 per cent substantive testing of auditee's data.

2.7 Controls play a more important role in IT environment than in the manual system. Auditors rely on assessment of controls to do their audit. However, the controls have changed in IT environment. So, as auditors we have to be aware of the impact of computer on the controls. In an IT environment, there are new causes and sources of error, which bring new risks to the entity.

General Controls

2.8 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[16]. Examples include IT policies, standards and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, business continuity planning, IT project management, etc.

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

- Organisation And Management Controls;
- IT Operation Controls;
- Physical Controls;
- Logical Access Controls;
- IT Acquisition Controls;
- Programme Change Controls;
- Business Continuity and Disaster Recovery Controls.

Application Controls

2.10 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 inputs, 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. Application controls include: Input, Processing, Output and Master/Standing Data Files controls.

[16] Information Technology Audit – General Principles, India.

Specific Controls

2.11 Specific Controls are peculiar to a particular environment and emphasis controls which are related to issues such as: network and internet, end user computing, e-governance, IT security and outsourcing.

PRELIMINARY EVALUATION

2.12 The first phase in audit viz. planning as explained in part I of these Guidelines should encompass preliminary evaluation of the computer systems covering:

- how the computer function is organised.
- use of computer hardware and software,
- applications processed by the computer and their relative significance to the organisation and
- methods and procedures laid down for implementation of new applications or revisions to existing applications[17].

2.13 In the 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 due to control deficiencies.

2.14 The results of preliminary assessments provide the basis for determining the extent and type of subsequent testing. If IT auditors obtain evidence at a later stage that specific control objectives are ineffective, they may find it necessary to re-evaluate their earlier conclusions and other planning decisions based on the preliminary assessment.

2.15 During the preliminary assessment phase of IT auditing, the IT auditor may gain an understanding of the entity's operations and identifies the computer related operations that are significant to the audit. This would also facilitate IT auditor in assessing inherent risk and control risk, making a preliminary assessment on whether general IT controls are likely to be effective and identifying the general controls that would require to be tested. A sample documentation of this understanding has been presented in Appendix 2.2

2.16 A sample survey questionnaire to solicit preliminary information from the auditee organisation regarding the primary features of IT Application is shown in Appendix 2.3.

AUDIT OF GENERAL CONTROLS

2.17 The IT auditor will focus on general controls that normally pertain to an entity's major computer facilities and systems supporting a number of different IT applications, such as major data processing installations or local area networks. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications i.e. Application controls.

[17] Information Technology Audit – General Principles, India.

2.18 The manual identifies critical elements that are basic and essential for ensuring adequate controls availability. The IT auditor may use the information for evaluating the practices adopted by auditee's organisation.

2.19 In order to facilitate the auditor's evaluation, sample audit programmes in a tabular format have been summarised in Appendix 2.4. These tables can be used for both initial evaluations as well as for documenting the auditor's work regarding the testing and audit procedures adopted for IT auditing while carrying out the control assessment work.

Organisational and Management Controls

2.20 These are the high level controls adopted by management to ensure that the computer systems function correctly and that they are satisfying business objectives. The aim of IT auditor will be to determine whether the controls that the auditee organisation has put in place are sufficient to ensure that the IT activities are adequately controlled. In carrying out an assessment, IT auditor should cover the following areas:

Control Objectives

IT Planning and Senior Management Involvement

- To ensure that in IT planning and implementation, there exists an active involvement of Senior Level Management so that IT is given the proper recognition, attention or resources it requires to meet business objectives. Also there exists a formal IT organisation structure with all staff knowing their roles and responsibilities, preferably by having written down and agreed job descriptions.

Formal Organisational Chart and Job Description

- To ensure that a formal IT organisation structure exists with all staff knowing their roles and responsibilities supported by clearly define job descriptions.

Personnel and Training Policies

- To ensure that organisation has controls and procedures in place to reduce the risk of mistakes being made. This may be achieved through the adoption of appropriate personnel policies and procedures.

Documentation and Document Retention Policies

- To ensure documentation maintained up to date and documentation retention policies should be in place in an organisation. When reviewing an organisation's system of internal control, the IT auditor can gain much of the information required from client documentation

Internal Audit Involvement

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

Legal and Regulatory Compliance

- To ensure compliance with the legal and regulatory requirements. This will vary from one country to another. Legal and regulatory requirements may include data protection and privacy legislation to protect personal data on individuals, computer misuse legislation to make attempted computer hacking and unauthorised computer access a criminal offence; copyright laws to prevent the theft of computer software

Segregation of Duties

- To ensure segregation of duties is a proven way of ensuring that transactions are properly authorised, recorded and that assets are safeguarded. Separation of duties occurs when one person provides a check on the activities of another. It is also used to prevent one person from carrying out an activity from start to finish without the involvement of another person.

Risk Areas

2.21 An IT auditor should be aware of the following critical elements[18]:

- Inadequate management involvement may lead to a direction-less IT function which, in turn does not serve the business needs. This may give rise to problems with the financial systems being unable to meet new reporting requirements (which may occur due a change in national accounting standards, or a change in government requirements);
- Poor reporting structures leading to inadequate decision making. This may affect the organisation's ability to deliver its services and may affect its future as a going concern (one of the fundamental accounting principles);
- Inappropriate or no IT planning leading to business growth being constrained by a lack of IT resources; e.g. the manager reports to the chief executive that the system is unable to cope with an increase in sales. Overloading a computer system may lead to degradation or unavailability through communication bottlenecks or system crashes;
- Ineffective staff who do not understand their jobs (either through inadequate recruitment policies or a lack of staff training or supervision). This increases the risk of staff making mistakes and errors;
- Disgruntled staff being able to sabotage the system, for example when staff find out they are going to be disciplined or make redundant;
- Ineffective internal audit function which cannot satisfactorily review the computer systems and associated controls;
- Loss of the audit trail due to inadequate document retention policies (includes both paper and magnetic, optical media); and
- Security policies not in place or not enforced, leading to security breaches, data loss, fraud and errors.

2.22 The organisation and management principles which are relevant to an IT function are the same as those within an organisation's finance function and such high

[18] ASOSAI IT Audit Training Material

level IT policies, procedure and standards are very important in establishing sound internal controls.

2.23 Management has ultimate responsibility for the safeguarding of the organisation's assets. They are responsible to stakeholders; taxpayers and citizens in the public sector. Management sets policies to ensure that the risks to the assets are adequately managed.

2.24 Management establishes and approves the policies. The policies are usually high level statements of intent. The policies may feed into standards. Detailed procedures (and controls) flow from the standards. It is important here that while reviewing an organisation's IT policies and standards, the auditor should bear in mind that each auditee organisation is likely to be different and have different organisational and management requirements. The auditor may assess whether the client's organisational structure and the place of IT within the structure is appropriate.

Audit Procedures

IT Planning and Senior Management Involvement

2.25 The roles and responsibilities of senior management in relation to their systems should be considered in audit. The auditor should review the high level controls exercised by senior management. An important element in ensuring that projects achieve the desired results is the involvement of senior management. Important considerations for auditor are whether a relevant committee are established involving senior management in computerisation project of the organization

2.26 This committee are involved in the formulation of Information Strategic Plan which should cover the following aspect:

- Effective management of information technology is a business imperative and increasingly a source of competitive advantage. The rapid pace of technological changes together with the declining unit costs, are providing organisations with increasing potential for:
- Enhancing the value of existing products or services;
- Providing new products and services; and
- Introducing alternative delivery mechanisms.
- To benefit from information technology requires: foresight to prepare for the changes; planning to provide an economical and effective approach; as well as, effort and commitment in making it happen.
- Information technology planning provides a structured means of addressing the impact of technologies, including emerging technologies, on an organisation. Through the planning process, relevant technologies are identified and evaluated in the context of broader business goals and targets. Based on a comparative assessment of relevant technologies, the direction for the organisation can be established.
- The implementation of information technologies may be a complex, time consuming and expensive process for organisations. Information technology planning provides a framework to approach and schedule, wherever possible, necessary information technology projects in an integrated manner. Through this process, performance milestones can be agreed upon, scope of specific

projects established, resources mobilised and constraints or limitations identified. Without effective planning, the implementation of information technologies may be misguided, haphazard, delayed and more expensive than justified.

- Good governance requires that all investments be justified — including any information technology investments. Information technology planning provides a process for not only evaluating alternative approaches, but also for justifying the selected approach in terms of benefits, both tangible and intangible, that will be realised by an organisation. This is an important dimension when many of the underlying projects may be difficult to support on an individual basis.

Personnel and Training

2.27 Staff employment policies should be adopted to ensure that appropriate staff are chosen. There should also be policies and procedures to deal with the other end of the employment cycle, i.e. termination (whether voluntary or compulsory). When emploting new members of IT staff, the organisation would be expected to take account of:

- *Background Checks*: including taking up references (in some countries it may be possible to check for criminal convictions);
- *Confidentiality Agreements*: these state that the employee will not reveal confidential information to unauthorised third parties; and
- *Codes of Conduct*: including contractual relationships with relatives, the acceptance of gifts, conflicts of interest etc.

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

- *Staff Assessment (including promotion and demotion)*: Staff assessment policies and procedures should be seen to be fair and equitable and understood by all employees. The policies should be based on objective criteria and consideration should be given to all relevant factors, which may include: the staff member's education, training, experience, level of responsibility, achievement and conduct.
- *Special Contracts*: It is increasingly common for IT departments to call in specialists, contractors and consultants for one off jobs. There should be policies which require those on special contracts to adhere to established policies and procedures
- *Job Rotation*: Job rotation can provide a degree of control because the same person does not carry out the same IT function all the time. Job rotation allows other staff to perform a job normally carried out by another person and can lead to the detection and identification of possible irregularities. Job rotation also acts as a preventive control. Staff are less inclined to adopt unapproved working practices or commit frauds if they know someone else is taking over the job.

Documentation and Document Retention Policies

2.29 The auditor may also need to examine client documentation to test check individual transactions and account balances. The policy on documentation should state that all system documentation should be kept up to date and that only the latest versions should be used. The policy may also state that backup copies of documentation should be stored in a secure off-site location.

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

2.31 Ultimately, if the organisation does not retain sufficient, appropriate evidence the auditor would have difficulty in being able to provide an unqualified audit opinion. The auditor should consider two types of documentation according to the audit approach:

- *Compliance Testing*: the auditor would require evidence of controls in operation during the accounting period. This evidence may consist of reconciliations, signatures, reviewed audit logs etc.
- *Substantive Testing*: assurance may require the auditor to examine evidence relating to individual transactions. The audit may need to be able to trace transactions from initiation through to their summarisation in the accounts. Where transaction details are recorded in computer systems they should be retained for audit inspection. If the organisation archives data, the auditor may need to ask for it to be retrieved before commencing the audit analysis. If the organisation summarises transactions into balances the auditor will need to find or request an alternative audit trail, e.g. asking the organisation to produce a hard copy of the transactions which make up the summarised balances.

2.32 There may be other non audit requirements which require the organisation to retain transaction documentation, e.g. specific requirements of legislations and regulations.

2.33 The organisation's documentation retention policies should take into account all such requirements.

Internal Audit Involvement

2.34 The external auditor may assess about the quality of internal audit's work acceptable, in terms of planning, supervision, review and documentation. The external auditor can view the organisation's internal audit function as part of the overall control structure (since they prevent, detect and correct control weaknesses and errors).

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

Legal and Regulatory Compliance

2.36 It may be assessed whether the organisation is aware of local requirements and have taken appropriate measures to ensure compliance.

Segregation of Duties

2.37 Evidence of separation of duties can be obtained 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.

2.38 The ability to apply and enforce adequate separation of duties is largely dependent upon the size of the IT department and the number of computer staff involved. Lack of segregated duties in a small computer department can be addressed by compensating controls, e.g. regular management checks and supervision, the use of audit trails and manual controls. However, in a large computer department the following IT duties should be adequately segregated:

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

2.39 In addition to segregated duties within the IT department, there should be no staff with dual IT department and finance department duties. The computer department should be physically and managerial separate from end users, such as finance and personnel. Segregation of duties reduces the risk of fraud since collusion would be required to bypass the control.

2.40 Separation of duties applies to both the general controls environment and to specific applications or programs. Within the general IT controls environment, the various functions and roles within the IT department should be segregated.

(**Appendix 2.5 shows a sample audit programme for evaluating Organisational and Management Controls.**)

IT Operation Controls

Control Objectives

2.41 The roles of IT operations include the following:

- *Capacity Planning*: i.e. ensuring that the computer systems will continue to provide a satisfactory level of performance in the longer term. This will involve IT operation staff having to make estimates of future CPU requirements, disk storage capacity and network loads capacity.
- *Performance Monitoring*: monitoring the day to day performance of the system in terms of measures such as response time.
- *Initial Program Loading*: booting up the systems, or installing new software.
- *Media Management:* includes the control of disks and tapes, CD ROMS, etc.

- *Job Scheduling:* a job is normally a process or sequence of batch processes which are run overnight or in background and which update files etc. Jobs are normally run periodically, either daily, weekly, monthly, quarterly or annually.
- *Back-ups and Disaster Recovery:* backups of data and software should be carried out by IT operations staff on a regular basis. Back-up and business continuity issues are covered in depth in a later session.
- *Help Desk and Problem Management:* help desks are the day-to-day link between users with IT problems and the IT department. They are the ones users call when they have a printer problem or they forget their password. Problems may be encountered with individual programmes (applications and system), hardware, or telecommunications.
- *Maintenance*: both hardware and software.
- *Network Monitoring and Administration*: The IT operations function is given the responsibility to ensure that communication links are maintained and provide users with the approval level of network access. Networks are especially important where the organisation uses EDI.

Risks Areas

2.42 The risks associated with poorly controlled computer operations are:

- *Wrong Applications Run, Incorrect Versions or Wrong Configuration Parameters*: e.g. the system clock and date being incorrect which could lead to erroneous interest charges, payroll calculations etc;
- *Loss or Corruption of Financial Applications or the Underlying Data Files*: may result from improper or unauthorised use of system utilities. The IT operations staff may not know how to deal with processing problems or error reports. They may cause more damage then they fix;
- *Delays and Disruptions in Processin*: wrong priorities may be given to jobs;
- *Lack Of Backups and Contingency Planning*: increases the risk of being unable to continue processing following a disaster;
- *Lack of System Capacity*: the system may be unable to process transactions in a timely manner because of overload, or lack of storage space preventing the posting of any new transactions; and
- *High Amount of System Downtime to Fix Faults*: when the systems are unavailable a backlog of unposted transactions may build up;
- *Unresolved Users' Problems*: due to a poor help-desk function. Users may attempt to fix their own problems.

Audit Procedures

Service Level Agreements (SLA)

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

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

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

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

Management Control, Review and Supervision

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

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

2.48 Management will be unable to provide continuous monitoring of operations staff and may place some reliance on the automatic logging and monitoring facilities built into the systems. The events which are recorded in the logs will depend on the parameters set when the systems were installed. As with most logging systems, a large quantity of data can be produced in a short period.

2.49 Recommending that an organisation review the audit logs on a regular basis is unlikely to be carried out in practice. To assist management in their detection of unauthorised activity, the organisation should develop procedures (e.g. a programme) to report exceptions or anomalies.

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

Training and Experience

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

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

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

Computer Maintenance

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

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

Operations Documentation

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

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

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

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

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

Problem Management

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

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

Network Management and Control

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

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

2.63 The IT auditor may be required to review the security and controls in non-financial systems and financial systems, depending on the scope of an audit and each SAI's mandate.

Physical Access Controls

Control Objectives

2.64 The objective of Physical Controls is to prevent unauthorised access and interference to IT services. In meeting this objective, computer equipment and the information they contain and control should be protected from unauthorised users. They should also be protected from environmental damage, caused by fire, water (either actual water or excess humidity), earthquakes, electrical power surges or power shortages. In IT arena, the second most likely cause of errors is natural disasters. The entity's IT security policy should include consideration of physical and environmental risks.

Risks Areas

Physical

- Accidental or intentional damage by staff.

- Theft of computers or their individual components (computer theft is on the increase and is likely to continue. Consider that, weight for weight, computer chips are worth more than gold and are very attractive to thieves);
- Power spikes or surges which may cause component damage and the loss or corruption of data;
- Bypass of logical access controls: e.g. having physical access to a fileserver can be exploited to bypass logical controls such as passwords; and
- Copying or viewing of sensitive or confidential information, e.g. pricing policies, pre-published results and government policies.

Environmental

- Fire/water damage (or damage from other natural disasters);
- Power: Cuts, leading to loss of data in volatile storage (RAM);
- Spikes: leading to system failures, processing errors, damage to components of equipment.
- Failure of equipment due to temperature or humidity extremes (or just outside tolerances of a few degrees);
- Static electricity: can damage delicate electrical components. Computer chips (ROM, RAM and processor) are delicate and easily damaged by static electricity shocks;
- Others: e.g. lightning strikes, etc.

2.65 Some of these risks are also covered in greater depth under the Business Continuity Planning of these guidelines.

Audit Procedures

2.66 To ensure that adequate internal controls exist to protect the business's assets and resources, the organisation should carry out a risk assessment. This would involve identifying the threats to the systems, the vulnerability of system components and likely impact of an incident occurring. Then he should identify counter-measures to reduce the level of exposure to an acceptable level. To do this, he must balance the risks identified with the cost of implementing controls. Some controls would be expensive to implement and would only be justified in a high risk environment.

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

Physical Controls

- Physical access controls are specifically aimed at ensuring that only those who have been authorised by management have physical access to the computer systems. Physical access security should be based upon the concept of designated perimeters which surround the IT facilities.
- Physical access controls reduce the risk of unauthorised persons gaining access to the computer equipment. The auditor should identify controls which would

restrict access to the organisation's site, the computer rooms, terminals, printers and data storage media. The organisation should also have considered the risks posed by cleaners, security personnel and maintenance staff. Common physical access controls include the use of locked doors, CCTV, intruder alarms, combination keypads and security guards.

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

Environmental Controls

- Computer installations should be protected against hazards such as fire, flood, power cuts, physical damage and theft. Inadequate protection increases the risk to system availability and ultimately an organisation's ability to produce a complete record of financial transactions. The organisation should have assessed the exposure to damage and introduced appropriate controls to reduce the risk to an acceptable level.
- The risk of fire damage can be reduced by the provision of fire detection and fire fighting equipment. Other measures, such as regular cleaning and removal of waste from the computer room, will reduce the risk of fire damage.
- The risk of water damage is largely dependent on the location of the computer facilities. Equipment located in close proximity to pipes and water tanks are at increased risk. Where possible, organisations should avoid locating computer equipment in basements or on floors immediately below or in the vicinity of water tanks. Automatic moisture detectors may be used to alert IT staff of potential water ingress.
- Computer equipment may be damaged or disrupted by fluctuations in the electrical power supply. Power surges can cause computer systems to delete or contaminate data. Uninterruptible power supplies reduce the risk of system disruption and damage and can allow continued processing following a power cut.
- Some of the older and larger computer installations require special environmental controls to regulate both the temperature and humidity in their vicinity. These controls usually take the form of air conditioning units. Many of the latest generation mini and micro computers have been designed to operate in an office environment and hence will not require special environmental controls.

Logical Access Controls

2.68 Logical Access Controls are defined as: "a system of measures and procedures, both within an organisation and in the software products used, aimed at protecting computer resources (data, programmes and terminals) against unauthorised access attempts."

Control Objectives

2.69 The objective of logical access controls is to protect the financial applications and underlying data files from unauthorised access, amendment or deletion. The objectives of limiting access are to ensure that:

- Users have only the access needed to perform their duties
- Access to very sensitive resources such as security software program, is limited to very few individuals and
- Employees are restricted from performing incompatible functions or functions beyond their responsibility

Risk Areas

- Users have the access to the areas other than related to the performance of their duties, causing threats to unauthorised access, amendment or deletion in the maintained data.
- Access to very sensitive resources such as security software program which may be of the mission critical nature and
- Employees are not barred from performing incompatible functions or functions beyond their responsibility.

Audit Procedures

2.70 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.

2.71 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 an organisation makes use of wide area networks and global facilities such as the Internet.

2.72 Logical access controls usually depend on the in-built security facilities available under the operating system (e.g. NOVELL Network) or hardware in use. Additional access controls can be gained through the appropriate use of proprietary security programs.

2.73 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. Organisations may be able to tailor the password system by, for example, setting minimum password lengths, forcing regular password changes and automatically rejecting purely numerical passwords, peoples' names, or words which appear in the English dictionary.

2.74 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 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.

2.75 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.

2.76 Significant risks are often posed by system administration staff with powerful system privileges. These 'super users' may have access to powerful system utilities that can by-pass established system controls. Management should have introduced measures to control the activities of these powerful users and, if possible, limit the system privileges of individual administrator to those required by their function.

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

2.78 The critical elements of an access control mechanism should include:

- Classification of information resources according to their criticality and sensitivity
- Maintenance of a current list of authorised users and their access privileges
- Monitoring access, investigating apparent security violations and take appropriate remedial action.

2.79 Resources, files and facilities requiring protection are:

- *Data Files:* These may consist of transaction files or databases. Any files containing master file or standing data information should also be protected, e.g. files containing payroll rates, bank account codes system parameters
- *Applications:* Unrestricted access increases the risk that the financial applications will be subject to unauthorised amendment leading to fraud, data loss and corruption. Unauthorised access to the source code of an application could be used to make amendments in the programming logic.
- *Password Files:* If these files are not adequately protected and anyone can read them there would be little to stop an unauthorised person obtaining the logon identification and password of a privileged system user. Any unauthorised user who obtained the access permissions of a privileged system user would be able to cause considerable damage.
- *System Software and Utilities:* These consist of software such as editors, compilers, program debuggers. Access to these should be restricted as these tools could be used to make amendments to data files and application software.
- *Log Files:* Log files are used to record the actions of users and hence provide the system administrators and organisation management with a form of accountability. A system log can record who logged onto the system and what applications, data files or utilities they used whilst logged on. An application log can be used to record changes to financial data (who changed what data, from what to what and when).

IT Acquisition Controls

2.80 The importance of IT related acquisitions is usually directly proportional to their cost, scale and complexity. In general, the larger and more complex the acquisition, the higher will be its impact on and importance to, the business. In addition, the acquisition may be important to the business due to its interrelationships with other IT projects.

Control Objectives

2.81 A structured acquisition process provides a framework for ensuring that:

- there are no major omissions from a business, technical or legal standpoint;
- the costs and resources for the acquisition process are appropriate and are efficiently deployed;
- the validity of the business case in support of the acquisition is reaffirmed prior to selecting a solution; and
- there is progressive buy-in to the new system as a result of user group involvement throughout the acquisition process.

Risk Areas

2.82 Critical elements involved in the process of acquisition of IT Assets are:

- The acquisition of IT is a key decision step in the life cycle of information systems. In many instances, the scale, cost and impact of an acquisition may have a strategic significance well beyond the acquisition itself. Also, any serious misjudgement in the acquisition decision will impair not only the success of the underlying IT project but, in addition, the potential business benefits that are anticipated.
- Acquisitions vary in scale, ranging from complex and pervasive new solutions for a mission-critical business area to the relatively straightforward acquisition of minor IT components to support an existing IT solution. Clearly, the more complex and pervasive the solution, the greater its importance to the organisation. Also, regardless of their size and complexity, IT acquisitions may be of significance due to either the potential interrelationships with major initiatives in the IT plan or the benefits associated with the acquisition.
- Acquisitions frequently involve a significant capital investment for an organisation. In addition to the investment, the opportunity cost of the capital employed and the time/resources expended in the acquisition process add to the importance of the acquisition.
- Some acquisitions may be of critical importance in meeting business objectives. For example, the acquisition may be essential in supporting a new product or service, or it may be the enabler in meeting business productivity or service level goals.
- The acquisition process provides a framework, including practices, procedures and monitoring mechanisms, that will ensure that there are no omissions in the process and that resources and costs associated with the acquisition are properly controlled. Also, the acquisition process is an opportunity to validate the

underlying assumptions of the business case to support the project as envisaged in the planning process.

- Finally, the acquisition process may provide an opportunity to gain organisation-wide consensus on the new IT project. This is possible due to the broad spectrum of management and users that are typically involved in an acquisition process. In this sense, early consensus will facilitate the ensuing implementation and change management process.

Audit Procedures

2.83 IT Auditor must ensure that the process adopted for acquisition of IT assets should encompass the following elements:

- adherence to a structured approach, comprising all the key acquisition activities and deliverables, timelines and milestones, project organisation and resources;
- enunciation of objectives, including a concise statement of the business expectations from the acquisition, detailed requirements and specification of overall scope;
- defined evaluation and selection criteria, particularly measurement scale, relative weights of all criteria and the manner in which acquisition and project risks will be minimised;
- commitment and support of executive management through a senior level project sponsor and, if appropriate, the establishment of an acquisition steering committee;
- participation from IT, users, consultants, legal and other interested parties, each with a defined set of responsibilities with respect to the acquisition; and
- compatibility with the organisation's acquisition policies and procedures, including any applicable regulatory guidelines.

Programme Change Controls

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

Changes may be requested for the following reasons:

- *Functionality Enhancement*: everyday system users may not be content with the functionality of the system. This could include discontentment with the screens they have, the system response time;
- *To Make Systems Operations Easier, More Efficient*: this category includes the tape/disk operators, the helpdesk manager, the database administrator and network management personnel;
- *Capacity Planning*: the system may require additional resources or increased capacity components.
- *Problems Rectification*: help-desk incidents leading to the identification of problems: each incident recorded on the Helpdesk will contribute to the

identification of underlying problems. If the problems are significant enough a request for change may be produced by the Helpdesk function;

- *To Improve Security*: IT security personnel : identified weaknesses in system security may result in requests for change which should improve security;
- *Routine Updates*: system developers may update and improve the system software; or
- *Changes in Requirements*: changes in legislation, business requirements or business direction may require the financial system to be amended.

Control Objectives

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

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

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

Risks Areas

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

Conversely the risks associated with inadequate change controls are:

- *Unauthorised Changes*: accidental or deliberate but unauthorised changes to the systems. For example, if there are inadequate controls application programmers could make unauthorised amendments to programs in the live environment;
- *Implementation Problems*: for example where the change is not in time for business requirements, e.g. annual tax rates;
- *Erroneous Processing and Reporting*: systems which do not process as intended. This could lead to erroneous payments, misleading reports, mis-postings of transactions and ultimately qualified accounts;
- *User Dissatisfaction*: systems which users are not happy with: this could lead to data entry errors, staff morale problems, a loss of productivity, union actions;

- *Maintenance Difficulties*: poor quality systems which are difficult or expensive to maintain (e.g. due to a lack of system documentation). Where there are inadequate controls over changes there could be multiple changes to the system so that nobody is sure which versions of software, or modules are being used in the live environment. Nobody would know which bugs had been fixed, or what parameters have been altered in different versions;
- *Use of Unauthorised Hardware and Software*: systems (hardware and software) in use which are not authorised. This could lead to incompatibility between different parts of the system, or breach of copyright legislation; and
- *Problems with Emergency Changes*: uncontrolled emergency changes to programs in the live environment leading to data loss and corruption of files.

Audit Procedures

2.89 It may be ensured in audit that the organisation's procedures to control changes should include;

- Procedures for management authorisation;
- Thorough testing before amended software is used in the live environment;
- The amended software is transferred or "transported" to the live environment only by or often authorised by operations management;
- Management review of the effects of any changes;
- Maintenance of adequate records;
- The preparation of fallback plans (just in case anything goes wrong); and
- The establishment of procedures for making emergency changes.

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

Business Continuity and Disaster Recovery Controls

Control Objective

2.91 The objective of having a Business Continuity and Disaster Recovery Plan and associated controls is to ensure that the organisation can still accomplish its mission and it would not loose the capability to process, retrieve and protect information maintained in the event of an interruption or disaster leading to temporary or permanent loss of computer facilities.

Risks Areas

2.92 The absence or existence of a well defined and tested Business Continuity and Disaster Recovery Plan may pose the following major threats to the very existence of the organisation itself in the event of a Disaster:

- The organisation's ability to accomplish its mission after re-starting its operations.
- To retrieve and protect the information maintained.
- To keep intact all the organisational activities after the disaster.
- To start its operations on full scale at the earliest to minimise the business loss in terms of money, goodwill, human resources and capital assets.

Audit Procedures

2.93 The organisation with computerised systems should have assessed threats to the system, its vulnerability and the impact a loss of operations would have on the organisation's ability to operate and achieve organisational objectives. Appropriate measures should then be put in place to reduce risks to a level that is acceptable to the organisation's senior management.

2.94 The extent of Business Continuity and 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 continuity and recovery plans which incorporate standby facilities at alternative sites. At the other end of the scale, a small agency or non-departmental public body with a desk-top PC, running a simple off the shelf package, would have a simpler plan.

2.95 Continuity and Disaster recovery plans should be documented, periodically tested and updated as necessary. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

2.96 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.

2.97 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.

2.98 The IT auditor while assessing the adequacy of business continuity and disaster recovery plan should consider:

- Evaluating the business continuity and disaster recovery plans to determine their adequacy by reviewing the plans and comparing them to organisational standards and/or government regulations.
- Verifying that the business continuity and disaster recovery plans are effective to ensure that information processing capabilities can be resumed promptly after an unanticipated interruption by reviewing the results from previous tests performed, if any, by the IT organisation and the end users.
- Evaluating off site storage to ensure its adequacy by inspecting the facility and reviewing its contents and security and environmental controls. It may be ascertained whether backups taken earlier have ever been tested for data recovery by the auditee organisation.

- Evaluating the ability of IT and user personnel to respond effectively in emergency situations by reviewing emergency procedures, employee training and results of their drills.

AUDIT OF APPLICATION CONTROLS

2.99 Application controls are specific to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance that all transactions are valid, authorised, recorded, and complete. 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 an organisation's accounts is correct or otherwise

2.100 Before getting on to audit 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;

- indicating the major transactions,
- describing the transaction flow and main output,
- indicating the major data files maintained, and
- providing approximate figures for transaction volumes.

2.101 Application Control requirements may be divided into:

- Input control
- Processing control
- Output control
- Master/Standing Data File control

Input Controls

Control Objective

2.102 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 authorised, 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.

Risk Areas

2.103 Weak input control may increase the risk of:

- Entry of the unauthorised data
- Data entered in to the application may be irrelevant.
- Incomplete data entry
- Entry of duplicate/redundant data.

Audit Procedures

2.104 The aspects that the auditor should evaluate are:

- all prime input, including changes to standing data, is appropriately authorised.
- for on-line systems, the ability to enter data from a terminal is adequately restricted and controlled.
- if there is a method to prevent and detect duplicate processing of a source document,
- all authorised input has been submitted or, in an on-line system transmitted and there are procedures for ensuring correction and resubmission of rejected data[19].

2.105 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.

Authorisation of Input

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

2.107 Computerised applications may be able to permit staff to enter and authorise transactions directly in the system. This can be achieved by setting up password access controls to data input devices and data entry permissions, e.g. data input screens. Financial applications may be able to check that a transaction has been approved by a person with the appropriate level of authority by checking their log-in ID against a predefined transaction approvals list.

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

- looking at access matrices;
- obtaining printout of user permissions;
- reviewing audit logs of changes in permissions;

Completeness of Input Data

2.109 As part of an IT audit, the auditor must determine if the accounting records are complete and that there are no material omissions. To do this the auditor should review the controls which ensure that input is complete, i.e. that transactions have not gone missing. The completeness of transaction input can be ensured by a variety of controls:

[19] Information Technology Audit – General Principles, India.

- *Manual Procedures*: e.g. keeping a log of transactions which users send for input. The data input staff in the IT department may expect a regular flow or pattern of transactions from user departments. Where a batch of input documents is expected but not received or a batch number appears to be missing, follow up action should be taken to identify the missing transactions;
- *Use of Pre-Numbered Data Input Forms*: These may be sequentially numbered. When a number is found to be missing the finance staff can investigate any disappearances. Alternatively the input transactions may be sent on sequentially numbered batch forms from user departments;
- *Use of Batch Totals*: In a traditional batch input system, all data is presented to the system in batches and incomplete batches are detected and exception reports are produced; and
- *Establishing a Routine or Expectation of Data Input*: e.g. If data entry staff expect to receive input documents from all 10 departments on a particular day and they only receive 9 sets, they would chase up the missing set of input documents.

2.110 The existence of batches is useful in establishing controls to ensure the completeness of input of data to the system. The total of individual transactions should agree to a manually calculated total recorded for input on a batch header document.

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

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

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

Data Input Validation

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

2.115 The accuracy of data input to a system can be controlled by imposing a number of computerised validity checks on the data presented to the system. Automated validation checks should be sufficient to ensure that all data accepted into the system is capable of acceptance by all subsequent processes, including acceptance into other systems where there is an automatic transfer of data. Acceptability is particularly important where feeder systems are used. For example the output from a standalone payroll system may provide the input for a general ledger system. Validation checks can reduce the risk of an application crashing because of logic errors arising when attempting to process input data with values outside pre-defined limits.

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

Duplicate Checks

2.117 The increase in the number of transactions that need to be processed has played a large part in the computerisation of accounting systems. Unfortunately, the increased volume of transactions has resulted in end user staff being less likely to remember transactions they have previously processed. This increases the risk that duplicate transactions will occur and remain undetected.

2.118 To address this risk, some applications may be able to detect duplicate transactions, e.g. by comparing new transactions with transactions previously posted to the same account. An IT auditor can make use of CAATTs software to detect the duplicate records in any transaction file.

Matching

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

Error Correction and Resubmission

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

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

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

2.123 *Held in Suspense*: In this case it is critical that users recognise the placing of items in suspense as a prompt for action. It is essential that all items held in suspense are corrected and ultimately successfully processed. In adopting this approach, we overcome the possibility of rejected items being lost but delay the recognition of the need to take action to correct the input error. Where items are held in suspense the auditor should review the procedures for identifying, correcting and clearing these transactions.

(**A sample audit programme for the evaluation of Input Controls is shown in Appendix 2.6**.)

Processing Controls

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

- adequately validating input and generated data,
- processing correct files ,
- detecting and rejecting errors during processing and referring them back to the originators for re-processing,
- proper transfer of data from one processing stage to another and
- checking control totals (established prior to processing) during or after processing.

Control Objectives

2.125 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[20].

Risk Areas

2.126 Weak process controls would lead to:

- inaccurate processing of transactions leading to wrong outputs/results.
- some of the transactions being process by the application may remain incomplete.
- allowing for duplicate entries or processing which may lead to duplicate payment in case of payment to vendors for goods.
- unauthorised changes or amendments to the existing data.
- absence of audit trail rendering sometimes the application unauditable.

Audit Procedures

2.127 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.

2.128 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,

[20] Information Technology Audit – General Principles, India.

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.

2.129 Computerised systems should maintain a log of the transactions processed. The transaction log 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 unclear transactions (such as part paid invoices). There should be procedures which allow identifying and reviewing all unclear transactions beyond a certain age.

(A sample audit programme for the evaluation of Processing Controls is shown in Appendix 2.7.)

Output Controls

2.130 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.

Control Objectives

2.131 Output controls ensure that all output is:

- produced and distributed on time,
- fully reconciled with pre input control parameters,
- physically controlled at all items, depending on the confidentiality of the document and
- errors and exceptions are properly investigated and acted upon.

Risk Areas

2.132 If output controls prevailing in the application are weak or are not appropriately designed these may lead to:

- repeated errors in the output generated leading to loss of revenue, loss of creditability of the system as well as that of the organisation.
- non-availability of the data at the time when it is desired.
- availability of the data to an unauthorised person/user.
- even sometimes, the information which may be of very confidential nature may go to the wrong hands.

Audit Procedures[21]

[21] Adopted from Information Technology Audit – General Principles, India.

2.133 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.

2.134 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.

2.135 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.

2.136 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.

(A sample audit programme for the evaluation of Output Controls is shown in Appendix 2.8.)

Master/Standing Data File Controls

Control Objective

2.137 Master/Standing Data File Controls are meant for integrity and accuracy of master and standing data files.

Risk Areas

2.138 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. Weak control in the system in maintenance of master/standing data files may lead to:

- unauthorised and uncontrolled amendments to the master and standing data files.
- unrestricted and uncontrolled physical and logical access to the application data files.
- poor documentation of the amendment procedures etc.

Audit Procedures

2.139 Auditors should see the following while examining the system:

- amendments to standing data are properly authorised and controlled.
- integrity of master and standing data files is verified by checking, control totals and periodic reconciliation with independently held records.

- amendment procedures are properly documented and controlled by management authorisation and subsequent review and
- physical and logical access to application data files are restricted and controlled.

AUDIT OF SPECIFIC CONTROLS

2.140 This section would focus on these specific controls that cover the following:

- Network control and use of the Internet including the risk associated with networks and network controls.
- End user computing controls including risks associated with end user computing and the associated controls.
- e-Governance
- IT Security Policy
- Outsourcing

Network and Internet Controls

Control Objectives

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

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

2.142 Opening up systems and connecting them to networks is not without its risks. The network should be controlled such that only authorised users can gain access control of networks is not just about logical access security and keeping out hackers. Networks are primarily used to transmit data. When data is transmitted it may be lost, corrupted or intercepted. There should be controls to reduce all these risks.

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

Risk Areas

2.144 Networks open up an organisation's computer systems to a wide, potentially anonymous user base. Where the organisation's systems are connected to networks there is potentially a greater risk of unauthorised access by outsiders (hackers) and non-authorised employees, leading to:

- *Data Loss*: data may be intentionally deleted or lost in transmission;

- *Data Corruption*: data can be corrupted by users or data errors can occur during transmission, e.g. a 1(in binary) is sent but due to interference, line noise etc, a 0 is received;
- *Fraud* : from internal and external sources;
- *System Unavailability*: network links and servers may be easily damaged. The loss of a hub can affect the processing ability of many users. Communications lines often extend beyond the boundaries of control of the organisation, e.g. the organisation may rely on the local telephone company for ISDN lines; wires may go through 3rd party premises;
- *Disclosure of Confidential Information*: where confidential systems such as personnel, or research and development are connected to networks there is an increased risk of unauthorised disclosure, both accidentally and deliberate;
- *Virus and Worm Infections*: Worm infections are specifically designed to spread over networks. Virus infections are very likely unless traditional protective measures such as virus scanning are continuously updated. Users tend to scan disks they receive from external sources but are less likely to scan data received over a network; and
- *Contravention of Copyright, Data Protection (Privacy) Legislation*: due to abuses by users of data or software available on the network or Internet.

Audit Procedures

2.145 Because of the nature of networks, physical access controls are of limited value. The physical components of the network (wires, servers, communication devices) must be protected from abuses and theft. However, the organisation must place great emphasis on logical access and administrative controls.

2.146 The logical access controls will vary from one organisation to another depending upon the identified risks, the operating system, the network control software in use and the organisation's network and communications policies.

2.147 Before carrying out a review of the organisation's logical access and network controls, the auditor should review any technical material or publications on the organisation's systems. For example, if the IT auditor happens to have a copy of a publication on security and controls for the organisation's network operating system, he should review it before visiting the organisation's premises.

2.148 Controls which the auditor may encounter include:

- *Network Security Policy*: this may be a part of the overall IT security policy;
- *Network Standards, Procedures and Operating Instructions:* these should be based on the network security policy and should be documented. Copies of the documentation should be available to relevant staff;
- *Network Documentation*: the organisation should have copies of documentation describing the logical and physical layout of the network, e.g. network wiring diagrams for security reasons, these are usually treated as confidential;

- *Logical Access Controls*: these are especially important and the organisation should ensure that logons. passwords and resource access permissions are in place;

- *Restrictions on the Use of External Links*: e.g. modems. These may be a weak link into the organisation's system, especially where the use of modems has not been approved the organisation may have decided to use call back modems. These are modems which only allow access when they call out. For example a remote user at home wants access to the system. He uses his modem to call the office. The office system connects and asks for an id code (and password), which the remote user enters. The office computer then disconnects. If the id code was correct the office computer dials backs on a pre-programmed number, in this example the home phone number of the remote user. The auditor should note that call back modems are not foolproof as their controls can be bypassed by call forwarding and other technical attacks. There are other controls which use a token (an electronic device with a identification feature) to confirm that the external user has permission to access the system;

- *Administration of Network*: The network should be controlled and administered by staff with the appropriate training and experience. Those staff should be monitored by management. Certain network events should be automatically logged by the network operating system. The log should be periodically reviewed for unauthorised activities;

- *Use of Network Management and Monitoring Packages and Devices*: There are many tools, utilities available to network administrators. They can be used to monitor network use and capacity. They can also be used to carry out inventory check on the software at each end user terminal;

- *Access by External Consultants and Suppliers should be Monitored*: It may be the case that the organisation has allowed the software supplier a remote access link to carry out maintenance and bug fixes. The use of this facility should be monitored and access only given when required and approved. The modem should only be activated when approval is given by the organisation's management and disconnected once the assignment is complete.

- *Terminals May Be Restricted to Pre-Defined Terminals*: This may be done via terminal codes, or Ethernet (IP) address;

- *Data Encryption*: In certain circumstances the organisation may encrypt data on the network. Even if an unauthorised user could tap into the line and read the data, it would be encrypted and of no use.

- *Use of Private or Dedicated Lines*: If the lines are private and dedicated to network communications there is a lower risk of data interception. Dedicated lines are also normally able to carry more data and are less likely to result in data transmission errors they also cost more; and

- *Use of Digital or Analogue Communication Links*: Digital links tend to have a higher capacity; they don't require modems and do not suffer from digital to analogue conversion errors.

Internet Controls

2.149 If you need to connect one of your computers directly to the Internet then the safest policy is to:

- physically isolate the machine from the main information system;
- assign an experienced and trusted administrator to look after the Internet machine;
- avoid anonymous access to the machine or, if it must be allowed, avoid setting up directories that can be both read and written to;
- close all unnecessary logical ports on the Internet server;
- monitor attempts to log in to the machine;
- transfer files between the main information system and the Internet machine only when they have been carefully checked and remembering that programs can be transferred in the body of mail messages; and
- have as few user accounts as possible on the Internet machine and change their passwords regularly.

Firewall

2.150 Sometimes the organisation needs to connect directly to the Internet outweigh the risks. In such cases it is usual to construct a "firewall" to help control traffic between the corporate network and the Internet. Firewalls consist of a combination of intelligent routers and gateway hosts. A router can be set up to allow only specific Internet services between the gateway and other specified Internet hosts. Software on the gateway host may provide additional services such as logging, authentication and encryption and packet filtering.

2.151 It is possible for an external computer on the Internet to pretend to be one of the computers on the corporate network. One particular function of the firewall is to stop any external packets that claim to be coming from the corporate network.

Password Policy

2.152 Authentication is the process of proving a claimed identity. Passwords are one means of authenticating a user. It is fairly easy for an Internet user to disguise their identity and their location. Stronger forms of authentication based on encryption have been developed to reinforce the authentication process.

2.153 A good password policy can make a significant contribution to the security of computers attached to the Internet. All the password policies previously mentioned in this chapter are applicable to systems with Internet connections, e.g. on password ageing, sharing, composition etc.

2.154 If users must log in over the Internet then it pays to use a challenge and response system as previously described.

Access Control

2.155 Every file on a computer connected to the Internet should have the minimum read, write and execute permissions consistent with the way that the file is used. UNIX password files are particularly sensitive as hackers are likely to take copies for later analysis. UNIX passwords are encrypted but there are readily available programs that will encrypt a list of words comparing each to entries in the password file. Since this can be done on the hackers own machine it will not trigger any alarms in the way that multiple unsuccessful attempts to log in should.

2.156 This attack is facilitated by the need for the etc/password file to be readable by everyone since it is read during the log in process. A partial defence is to use shadow password files and a modified login program. Using this approach the shadow password file can be protected whilst the etc/password file contains no real passwords. Another defence is to use a non-standard encryption algorithm.

Encryption

2.157 Two forms of encryption are widely used:

- symmetric encryption uses the same key for encryption and decryption; and
- asymmetric encryption involves generating a pair of keys which are known as the public and private keys.

2.158 Symmetric encryption is fast but makes key distribution hard whereas asymmetric encryption is slow but does not suffer from the key distribution problems. A combination of the two approaches may provide the best solution.

End User Computing Controls

Control Objective

2.159 The term end user computing refers to the situation where users have intelligent computers on their desktops (i.e. computers with their own CPU processing capabilities), together with applications which allow them to develop their own processing and reporting systems. End user computing has given users greater control over the processing and presentation of their data. Conversely, end user computing has reduced the control exercised by central IT departments.

Risks Areas

2.160 From the beginning, developments in end user computing environments have been uncontrolled. Users do not adopt the same standards or good practices that their colleagues in the IT department use. This uncontrolled environment can and has led to a waste of time, effort and money for the organisation. The fact that end user computing has been so uncontrolled also causes the auditor concerns, especially where critical transactions are processed by end users.

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

System Development

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

- what standards the systems should be developed to;
- what documentation is required;
- what controls should be built into the new system; and

- what testing is necessary to ensure that the system does what it is supposed to do.

2.163 End user computing has permitted end users to develop their own applications without assistance from central IT departments. The end users developing their own systems do so without the relevant skills and training. When you have systems being developed in the absence of standards, by non-experienced or trained staff you invariably get problems. Typically these include:

- *Unreliable Systems Which Do Not Process Data in the Way Intended*: e.g. the underlying logic of the applications has not been thought through or coded correctly;
- *Systems Which Do Not Include Basic Data Integrity, Input, Processing or Output Controls*: e.g. example financial accounting systems which accept single sided double entries, resulting in unbalanced trial balances;
- *Systems Which are Untested and Unpredictable*: e.g. if the system has not been tested to ensure that it can deal with incorrect data input it may crash or hang when such data is entered by a user;
- *Systems Which are Not Documented*: This makes it difficult to maintain the system in the longer term. IT auditors have frequently heard organisations tell them that an application was developed by an employee five years ago and since that person left no-one has been able to find any documentation to enable them to understand exactly how it works;
- *Systems Which Have Been Subjected to Uncontrolled Change*. End users have a habit of diving in whenever they find a problem in their own applications. They tend not to follow the same change control procedures as used in IT departments. This leads to changes which are poorly thought out and programmed. These changes may have a detrimental impact on the system. For example, a user may change a formula in a table and unknown to him/her it has an unplanned knock on effect elsewhere;
- *Incompatibility and Fragmentation of Information*: the systems purchased by end users may be incompatible with the corporate systems. This makes on-line sharing of data difficult to achieve. Data on end user systems may not be up to date and include the latest amendments to the data on the central system.

Duplication of Effort

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

Data Inconsistencies

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

- Data inconsistencies are likely to be greater where the organisation uses a distributed system.
- Data inconsistencies can cause the auditor problems if different parts of an organisation use different standing or master file data in their calculations, e.g. pay rates for sub-contract staff or unit costs for sales invoices or overhead apportionment rates for the calculation of full costs.

Increased Use of Resources and Costs

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

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

Erasure of Central Information

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

Loss of Data

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

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

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

Logical and Physical Access Security

2.172 The majority of personal computers use the DOS, Windows 95, Window 2000, Window NT, OS/2 or Macintosh operating systems. These operating systems are designed for single users and consequently have little in the way of logical access controls to restrict access to unauthorised users.

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

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

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

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

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

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

Audit Procedures

Systems Development Controls

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

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

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

Duplication of Effort

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

Data Inconsistencies

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

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

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

Legislation

2.186 The organisation should establish policies to ensure that end users are aware of and comply with relevant legislation. The awareness program may cover:

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

Data Loss

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

2.188 Control procedures could include:

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

Logical and Physical Access

2.189 Users should be encouraged to adopt at least basic logical access security precautions on their standalone personal computer, e.g. setting the BIOS password. If possible, data should be stored on network fileserver. In general the network operating system will provide a degree of protection against unauthorised access via the network.

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

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

End User Support

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

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

Protection against Computer Viruses

2.193 There are a number of controls that an organisation could put in place to reduce the risk of viral infection. Some are technical in nature other are administrative and procedural. Staff should be made aware of the risks and informed of the measures adopted by the organisation to manage the risk.

Use of Anti-virus Software

2.194 There are many products on the market which claim to detect computer viruses. The software should be supported by a screening policy. The policy should require all incoming media to be scanned for viruses before it is loaded onto a computer.

2.195 Anti-virus software may be installed on every computer or alternatively one could be set up as a standalone "sheep-dip" computer. Ideally the anti-virus software should be as transparent to the users as possible, i.e. it should be unobtrusive.

2.196 Some anti-virus software only scans when prompted by the user. Others provide continuous protection by loading a TSR (terminate and stay resident) program into memory. TSR anti-virus programs keep a constant lookout for viruses and run as a background program.

2.197 However, the anti-virus software runs the risk of always being one step behind the virus writers. Even where anti-virus software is used there may be a new virus which the software cannot detect. This makes regular updating of the virus scanners very important.

Back-ups

2.198 It is very important that organisations regularly back up their computer files. Back-ups can be made less onerous by using automatic backup software.

e-Governance

2.199 The Internet and related technologies are transforming the world we live in. They are a growing influence on the way individuals, not- for-profit bodies, businesses and governments communicate and operate.

Control Objective

2.200 E-government focuses on capturing the benefits of internet and related technologies to improve the efficiency and effectiveness of government services.

Risk Areas

2.201 Implementing an e-Governance project is not just implementing any IT project but would involve the component of business process re-engineering in the Government business. Security consideration would be high in an e-Governance initiative because of the involvement of Internet delivery mechanisms and data transmission over networks. It involves the risks of unauthorised access of data, hacking of data; much faster virus spread problems etc. as it may extend to the extent of Electronic Funds Transfer etc.

Audit Procedures

2.202 While taking up IT Audit of an e-Governance project, following aspects should be analysed in audit depending upon the audit scope and audit objectives:

- Strategic Planning
- Vision and priorities set out by the top management
- Funding and costs
- Confidentiality and Security of data
- Legal Requirements
- Project Management
- Performance Measurement criteria adopted by the organisation
- Ease of Interface use
- Social Inclusion/Exclusion
- Benefits accrued – social and economic
- Sustainability of project
- Appropriate Technology Adoption

IT Security Policy

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

Control Objectives

2.204 By way of enunciating an IT security policy, the organisation:

- demonstrates its ability to reasonably protect all business critical information and related information processing assets from loss, damage or abuse;

- aims to enhance the trust and confidence between organisations, trading partners and external agencies as well as within the organisation;
- assures conformity to applicable contractual and regulatory requirements.

Risk Areas

2.205 Absence or existence of a weak IT security policy in an organisation may exclude the following basic principles of information security:

- Responsibility and accountability must be explicit
- Awareness of risks and security initiatives must be disseminated
- Security must be addressed taking into consideration both technological and non technological issues
- Security must be coordinated and integrated
- Security must be reassessed periodically
- Ethics must be promoted by respecting the rights and interests of others
- Security must be cost effective
- Security procedures must provide for monitoring and timely response

Audit Procedures

2.206 There should be specific statements in an IT security policy indicating minimum standards and compliance requirements for specific areas like (i) assets classification, (ii) data security, (iii) personal security, (iv) physical, logical and environmental security, (v) communications security, (vi) legal, regulatory and contractual requirements, (vii) business continuity planning, (viii) security awareness and training, (ix) security breach detection and reporting requirements, (x) violation enforcement provisions, etc.

2.207 There are two basic level controls in an IT security policy – physical controls restrict individual physical access to IT resources and logical controls restrict access to specific systems to authorised individuals and to the functions each individual can perform on the system. It would be evident that many of the specific issues in IT security would be covered in this manual under coverage of various internal control objectives. Nevertheless, the aspect of IT security is gaining ground and is being emphasised more frequently than before due to the strategic importance of data, reliance on data for decision making and confidentiality of data requirements.

2.208 IT security policies are normally expressed in the form of a concise narrative, i.e. a few pages of text. The policy requires senior management approval if it is to have any weight and consequently should be approved at board level or equivalent. The policy should be seen to be backed by senior management. The policy should be available to all employees responsible for information security.

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

2.210 It is also important that information security implementation in an IT application takes care of:

- Confidentiality of data meaning thereby that data or information is accessible only to those authorised to have access;

- Integrity, so as to safeguard the accuracy and completeness of information and processing methods; and
- Availability of data to authorised users and on time.

2.211 The objective of data security is "the protection of the interests of those relying on information and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity."

2.212 The concept of security applies to all information. Security relates to the protection of valuable assets against loss, disclosure, or damage. In this context, valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure. The protection is through a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

2.213 Many of the general and application controls are aligned with the above objectives of securing data as organisations may incur huge losses due to data loss.

2.214 An auditor can make extensive use of CAATTs software to test the integrity and completeness of data as outlined in part IV of this manual. Such substantive testing of data may need to be done by IT auditor for assessment of data reliability in case the controls implemented in IT organisation are found to be dissatisfactory.

Outsourcing Policy

2.215 There is an increasing trend for IT services to be delivered by third party service providers. This has arisen because IT is not seen as being a core business activity. By the late 1990s, IT outsourcing had become a mainstream management option and outsourcing contracts are now quite common in auditee organisations. Management may take the attitude that their business involves the delivery of products and services and not the provision of IT services.

Control Objective

2.216 Outsourcing allows management to concentrate their efforts on the main business activities as the need for developing and maintaining the IT systems are taken care of by third parties.

Risk Areas

2.217 The decision of outsourcing any business activity, may have the basic intentions of allowing the Top Management to concentrate more upon the main business activities, however, this involves invitation to the risk of allowing a third party to have access to the business secrets, important data and other related facts.

Audit Procedures

2.218 Where an organisation outsources or intends to outsource its IT activities the auditor should be concerned with reviewing the policies and procedures which ensure the security of the organisation's financial data. The auditor may need to obtain a copy of the contract to determine if adequate controls have been specified. Where the organisation intends to outsource its IT function the auditor should ensure that audit needs are taken into account and included in contracts. Contract terms are frequently difficult to change once they have been signed. Even if the third party is willing to amend the contract it is likely to charge a large fee for doing so.

2.219 Organisations, particularly those in developing countries and those with little relevant previous experience, may inadvertently create various problems when they decide to outsource their system development and software implementation projects. These may include:

- The price of the software to be implemented often appears to be the deciding factor in choosing the outsourcing vendor rather than the overall potential result for the organisation.
- The organisation generally has little or no clear plan of what it wants done. There are no clear ideas on reporting requirements and, at times, very little in the way of specified or defined systems. Most of the time, the development work is undertaken with systems, procedures and controls evolving alongside.
- Management does not really know what platforms may be best suited for the proposed development work.
- Top management is, or regards itself as being, too busy to be trained in the software to be used. This has a debilitating effect on the rest of the staff. Success of the project depends on significant participation by top management.
- Where activities are outsourced, management and users may sometimes expect far more than is really possible. They may have an unrealistic expectation of the value to be expected for the payment being made. For example, even though the basic payroll or accounts may be produced in a timely and cost-effective fashion, users may also expect complex and unspecified information reports that, in fact, are not produced and never could be for the contract price of the service.

2.220 The IT auditor should also focus on issues related to Intellectual Property Rights and evaluate whether the programmes developed by outsourcing components to a third party are duly protected as per contract terms and are not prone to outside use by other organisations.

PART 3 INFORMATION SYSTEM DEVELOPMENT AUDIT

INTRODUCTION

3.1 Historically, system development projects have often been undertaken by, or under the dominance of an organisation's IT department. In such a scenario there is very little or no end user involvement, and consequently the system delivered often fails to meet its end users' expectations in full. This will result in the organisation failure in reaping the full benefits on its investment. It is now widely accepted that the system's eventual owner and its end users must be identified before the project commences so that their needs are taken fully into account. Good quality end users should be assigned to the project team at an early stage and where possible, the project should be under the overall control of a director or senior manager from the end user side.

3.2 Therefore it is very essential that auditors as one of the users of the system to be involved in this process. The auditor will have to acquire good understanding of the system development methodology employed as well as identifying the pertinent controls in the development process to ensure that the audit requirements and the information technology strategic plan of the organisation is achieved. To satisfy the above objectives, the auditor will either be involved during the development of the system or during the post audit review on developed system.

3.3 The pro-active involvement of auditor during the system development phase, known in this manual as the Ongoing Project Audit, will add value to the development process particularly on aspects of internal controls, system security, and ensuring that the audit requirements for the system is incorporated. However, it is important not to misconstrue the auditor involvement here as compromising his/her independence. The auditor involvement should abide to the INTOSAI Auditing Standards on Independence.[22]

3.4 In performing the Ongoing Project Audit, auditors will participate throughout the development process which involved assessment of risks and reviewing of deliverables throughout the process. Input from auditor on aspects of internal controls, security, project management and compliance with requirements and quality standard is brought to the direct attention of the project team for considerations. The advantage of auditing before completion is that there may still be opportunity to turn bad project into an acceptable one or to stem the losses from a project that cannot possibly deliver the value expected.[23]

3.5 In Post Implementation Audit, auditors will evaluate the specific system after it had been implemented. The evaluation done will include the overall project management, and controls over the development process of the system encompassing reviewing the funding, approval process and the role of central agencies in monitoring the system under development. This audit can also be extended to include the evaluation of system effectiveness and efficiency. The lessons learned from this

[22] Paragraph 2.2.25 to 2.2.29, INTOSAI Auditing Standards On Independence. (Excerpts in Appendix 3.1)

[23] OAG of Canada, Lead Paper: System Development Audit at theOAG proceedings from the INTOSAI Standing Committee on EDP Audit 2nd Working Seminar, 1998

exercise will provide useful input for improvement in future development and the maintenance of the system.

AUDIT OBJECTIVES

3.6 The audit objectives for both the Ongoing Project Audit and the Post Implementation Audit is the same.

3.7 The objective of the audit is to ensure that the development process is in compliance with the prevailing policies and regulations; the overall project management and controls over development of the system are satisfactory, pertinent and sufficient internal control and audit trails are in place; the quality of the system development is maintained and the system ultimately support the strategic objective of the organisation as well as meeting the needs of the users.

PROJECT MANAGEMENT

3.8 A sound project management adopted during system development on IT based system will determine the success of failure of the project. INTOSAI Study Committee on EDP Audit[24] identified several factors which contribute towards projects failure such as:

- Shortage and quality of IT staff
- Misunderstanding between the various parties involved in the process with regard to their roles and the understanding of the projects and concepts being used.
- Insufficient participation from end-users, particularly for project issues which different departmental boundaries in the department or agency.
- Senior managers must have both responsibility and accountability and sound business knowledge, and be aware of the opportunity and risks of IT. The managers need to find a balance between the need of business process re-engineering and an IT solution.
- Project managers must have the right skills and experience and stay throughout the lifetime of the project, and there is a shortage of such staff. It is important to bring in other knowledge, e.g. engineering knowledge, of how to conduct building projects.
- Risks must be identified and managed (include culture and change management issues).

3.9 Auditor will examine the effectiveness of the project management methodology adopted by the organisation in executing this project plan. Among the component to be evaluated are: project organisation, the nature and extent of responsibilities, authority and accountability of the project management, empowerment of the various parties, the effectiveness of the team leader and the usage of resources.

[24] Proceeding of the INTOSAI Standing Committee on EDP Audit , 3rd Working Seminar on Performance Auditing in IT Environment, May 14-16, 2002, Ljubljana, Slovenia.

RISK MANAGEMENT

3.10 The overall objective of the audit in system development is to contribute to the success of the system project. To ensure that the system under development will achieve a satisfactory conclusion, the organisation should focus on risk management of the project. Turban [25]et al suggest four phases of risk management of project as follow:

- *Assessment Phase*: Organisation evaluates their security risks by determining their assets, threats, and vulnerabilities.
- *Planning Phase*: Established security policies to define threats (tolerable and intolerable threat). A threat is tolerable if the cost of safeguard is too high or the risk is low. The policies also specify the general measures to be taken against those that are intolerable or a high priority.
- *Implementation Phase*: Specific technologies are chosen to counter high-priority threats. The selection of particular technologies is based on the general guidelines established in the planning phase.
- *Monitoring Phase*: A continuous process used to determine whether measures are successful or not and need modification; there are any new types of threats; there have been advances or changes in technology; and whether there are any new business requirements with potential risk exposure.

3.11 Basically the auditors' role is to identify the risk exposure and evaluate the operability, completeness and sufficiency of the risk management plan establish by the organisation. The two types of risk exposures in system development are:

- Security risk exposure stem from inadequate built-in automated control designed to validate data processing; to restrict access to data, ensure a sound separation of roles and to monitor system usage; and to provide appropriate business continuity
- Project risk exposure relates to the financial justification for the project, and includes such impact as late delivery, cost over-runs, failure to deliver the anticipated business benefits and premature obsolescence.

3.12 Appendix[26] 3.2 summarised the risk exposures breakdown into a number of detail risk. Listed below are factors which are essential ingredients for successful project management:

- There must be clear and concise statement of what the project is setting out to achieve and this must be understood and accepted by all the stakeholders.
- It is essential to identify who the eventual customer of the project's deliverables is. The customer is the main beneficiary of the project and will have an important role in agreeing with the project goal and providing essential support.
- An effective change management system is essential to safeguard projects from uncontrolled changes.

[25] Turban, E et al, Electronic Commerce, *A Managerial Perpective - Electronic Commerce*, Prentice Hall 2002

[26] INTOSAI's Student Notes on Auditing Developing System

- For successful project management an effective project organization should be created with proper definition of roles, responsibilities and reporting lines.
- A properly used project management methodology will promote the successful establishment, operation and closure of a project.
- All risks associated with projects should be identified and appropriately managed.
- Since projects very often form business relationships between groups of people who normally do not work with each other, appropriate team building measures should be adopted. Openness and honesty should be encouraged so that problems are not disguised.
- Projects involve movement from one system to another and hence a clear transition strategy is essential to a project's success.
- It is essential to have an experienced project manager with sufficient status in the organisation.

FUNDING

3.13 All system development should be subjected to budgetary controls to ensure resources are adequately allocated and to allow for benchmarking to be made for progress and cost of project against funding. Therefore, accurate estimates of timescales and resources are essential ingredients of any realistic plan. Ideally all project stakeholders should be involved in either preparing or reviewing estimates/funding. Those involved in the preparation of estimates must be given authority and backing to obtain the information required about the project needed to perform the estimating task. They should:-

- become familiar with the proposed system;
- be aware of the environment in which the proposed system is to be produced/developed;
- prepare the estimate, using the appropriate estimating models and techniques (e.g. expert judgement - possibly based on the moderated view of a group of experts; analogy with similar projects);
- assess the effects that factors in the local development environment may have on the estimates;
- advise the Project Manager how to interpret the estimate, including the various risks;
- re-estimate as the project proceeds and when more accurate estimates are possible

3.14 The audit review will include the use of realistic estimate to complete tasks and the effectiveness of the project team and the usage of resources.

DELIVERABLES

3.15 It is important to ensure that a team is working on the most appropriate tasks by building a detailed schedule and sticking to it to ensure that the project will complete on time. Auditor should assess the milestone achieved against the implementation schedule to ensure promptness and consistency of time reporting and the completion of task and deliverables.

3.16 Listed below are the Project Scheduling Principles[27] that could be considered in defining the deliverables during the system development:

- *Compartmentalisation*: The product and process must be decomposed into a manageable number of activities and tasks.
- *Interdependency*: Tasks that can be completed in parallel must be separated from those that must be completed serially.
- *Time Allocation*: Every task has start and completion dates that take the task interdependencies into account.
- *Effort Validation*: Project manager must ensure that on any given day there is enough staff members assigned to complete the tasks within the time estimated in the project plan.
- *Defined Responsibilities*: Every scheduled task needs to be assigned to a specific team member.
- *Defined Outcomes*: Every task in the schedule needs to have a defined outcome (usually a work product or deliverable).
- *Defined Milestones*: A milestone is accomplished when one or more work products from an engineering task have passed quality review.

3.17 In a phased methodology of system development each phase represents a milestone on that certain objectives should have been met, decisions made, data gathered or analysed.

ADHERENCE TO STANDARDS

3.18 The auditor should ensure that deliverables at each phases of the implementation is clearly defined in advance so that it could be easily evaluated in terms of quality assurance, timeliness, relevancy and completeness, and more importantly as a benchmark against which project can be measured.

3.19 SDLC standards provide procedural controls over development of new system. It will involve a series of stages throughout the development process where an authorisation is required at each stage along with a review of progress.

3.20 Auditors could assess the consistency of practices and standard employed with regard to the various phases of the system development vis-à-vis initiation, system analysis and specification, system design, system development, acceptance testing, implementation and post implementation review. **Figure 1** below shows the life cycle responsibilities of the various groups and their deliverables.

[27] Pressman, R.S, "Software Engineering – A Practitioner's Approach", Mc Graw Hill, 5th Edition (pg. 169-170).

FIGURE 1 - Life-Cycle Responsibilities

Development Phase	Lead Responsibility	Output
Initiation	User	Will recommend for endorsement or abandonment of the proposal (recommendation – include identifying a suitable solution to the problem and seeking approval from the relevant authority. Business case - to provide full justification and to be reviewed continuously
System Analysis	User	Will produce requirements and specifying accurately and comprehensively users requirements statement
System Design	User/IT Department	Data flow diagram, Logical data structure and the conceptual model of the logical process. Maps the logical design into the implementation environment (operating system, DBMS, Hardware etc)
System Development	IT Department	Coding and development testings
Acceptance Testing	User/IT Department	System roll-out and commissioning
Implementation\Maintenance	IT Department	User manual, technical specification etc
Post Implementation Review	Independent group	Evaluation and recommendation

SYSTEM DEVELOPMENT METHODOLOGY

3.21 The auditee's organization should adopt a methodology to ensure that systems are implemented using technique designed to provide effective systems without taking unacceptable risks that would jeopardize the auditee's operations.

3.22 It is important for the auditor undertaking this audit to be aware of the various types of development methodology that could be adopted by the auditee's organisation. That being the case, auditor should be familiar with the controls and standard over the development process based on the methodology adopted by the auditee's organisation.

3.23 The most established and standard methodology known as the System Development Life Cycle (SLDC) involves common activities describe below:

- Performing the feasibility study;
- Identifying users' requirement;
- Identifying and evaluating alternatives;
- Transforming user requirement into system specifications;
- Preparing the system design for development;

- Conducting the various types of testing – such as unit, integration and eventually acceptance testing;
- Rectifying problem encountered;
- Preparing the various types of documentation - such as end user and system documentation;
- Implementing the new system for life operation; and
- Performing the post implementation review (PIR) where feedback will serve as input for the system maintenance

Initiation Phase

3.24 During the Initiation Phase, the justification for the need for an IT based solution to a problem is identified, quantified and confirmed.

3.25 The organisation should prepare a clear, convincing, well supported by evidence and fact based business case. This document will help to convince the relevant authority that the project will bring real benefit to the organisation before endorsing it. A standard business case[28] should include the following:

- why the system is needed;
- the business objectives to be met or enhanced;
- any long term business implication;
- any staff and organisation implication;
- the alternative options which were considered;
- the recommended option;
- any important assumptions that have influenced recommendation;
- when the system can be delivered;
- its overall priority among other impending projects;
- the benefits to be delivered by the system;
- the risk of not delivering the benefits;
- the risks involved in pursuing the project;
- an investment appraisal;
- outline cost and plans for the project

3.26 The objective of the initiation stage is to underline the groundwork for future management of a project and to obtain approval for its commencement. Initiation might relate to a study to the entire project, or to a single stage of a project. Therefore initiation stage might occur at a number of stages in the system development. The following areas need to be addressed during the initiation stage:

- the scope of the project;
- appointment of project team and quality assurance team;

[28] INTOSAI's Student Notes on Auditing Developing System

- appointment of staff and consultancy support;
- training needs before project commences;
- any options raised in earlier report (Project Initiation Report)
- continuing validity of the existing user requirements, and any assumptions and recommendations;
- the identification and management of both business and security risk

3.27 In conducting the audit review for the Initiation Phase, the auditor will have to communicate directly with the project team. He/she well identify those deliverables that have direct impact to either proceed or discontinue the project. These deliverables should be evaluated rigorously to allow the auditor to form an opinion on the reasonableness of the decision taken related to the system. The prominent deliverables at the Initiation Phase are:

- The Needs Statement which include an expression of the need in terms of an organisation strategic plan, problem areas, reforms or process re-engineering proposed and alternatives, opportunities in improving economy and efficiency, the internal control and security needed for the system.
- The Feasibility Study which include an analysis of objectives, requirements, and system concepts, an evaluation of alternative approaches and a description of the proposed approach.
- The Risk Analysis which include the identification of internal control and security vulnerabilities, the nature, magnitude and safeguards of associated threats and assets covered by the proposed system, and a detailed review of all data and assets to be processed or accessed by the system.
- The Cost/Benefit Analysis which include the cost to build the system, system benefits, impact to system internal control and security etc.

System Analysis

3.28 The real start of any development project is the system analysis phase or also known as **Definition of Functional Requirements**. The activities involve in this phase include interviewing users, reviewing existing documentation, defining data, and modelling the data and processes that define the functionality of the system.

3.29 To avoid system inefficiency and delivery delays, it is important that the users' requirements are fully captured and understood in order to avoid changes and/or new requirements emerging at later stages.

3.30 During the system analysis phase, the auditors will evaluate whether end users needs are well defined and transformed into requirement definitions. Basically, the deliverables at this phase are:

- The user requirement statement which capture the needs from the various users.
- The Functional Requirements Document which includes the detailed information on the system input screen layout, coding the automated process, interfaces, output format and the controls and the security requirements.
- The Data Requirement Document which defines the detailed description of the data require as input and output, data logical groupings, characteristics of each

data element, the procedures for data collection, and description for sensitive and critical data.

System Design

3.31 In design and development phase, the logical data and process models which were created during the analysis process are used to create the physical design of the system. This phase is concerned with how the functional requirements will actually be provided and provides a definition for the programmers who will go on to build the system.

System Development

3.32 Once the program and database specifications are completed, they must be translated into the commands and instructions required by the computer to run the system. There are a variety of ways in which this can be done ranging from the traditional writing of a string of program instructions to newer techniques which include Rapid Application Development (RAD), Case Tools and Object Orientation Programming.

3.33 The development phase also includes the testing which must be carried out to ensure that the system is operating as required by the functional requirements. Various levels of testing will be carried out including:

- Unit testing: to ensure individual program modules function correctly.
- Integration testing: to ensure that related program modules work together.
- System testing: to ensure that the whole system works as required.
- Acceptance testing: the final test by the users to ensure that the system actually does what they wanted in the first place.

3.34 The deliverables developed at the end of this phase are:

- User manual which describe the functionality of the system in non-technical terminology.
- Operating manual provide IT staff with a description of the system and the operational environment.
- Maintenance manual provides technical staff with the information and source codes necessary to understand the program, their operating environment, their maintenance procedures and security requirements.
- The verification and testing plan which includes all testings done (mentioned in paragraph 3.33 above) supported by the test results.
- Migration Plan describes the installation or implementation of the system for system roll-out. This document is used after testing of system, including security and internal control features have been carried out.

3.35 The auditor should evaluate the adequacy of the documentation, the coding and their testing efforts carried out.

Implementation and Maintenance

3.36 This phase involves the migration from existing system to new system. This will take place after the users are satisfied that the system has undergone successful testings and the auditee's organization has signed off.

3.37 It is during this stage where the actual operation of the system in a production environment is seen. Problems/issues related to violations of system security, backup plan, business continuity plan, standing data file integrity and other programmes malfunctions will be taken up for maintenance.

3.38 The deliverables developed at the end of this phase are:

- Migration Plan which will elaborate of the cutover method adopted and the controls over data transferred to new system;
- Report on problems which require maintenance; and
- Corrective measures to tackle the problems identified earlier supported by the appropriate documents.

Post Implementation Review

3.39 A Post Implementation Review (PIR) is the final stage of a system development project. Its aim is to establish the degree of success achieved by the development project and to determine whether any inputs can be applied to improving the organisation's development process. The full scope of a PIR will depend largely on the scale and complexity of the project. Overall it should establish in an impartial manner whether a new system has met its:-

- business objectives (delivered within budget and deadline; is producing predicted savings and benefits, etc.)
- user expectations (user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.);
- technical requirements (capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.).

3.40 During the PIR it is also important to identify any lessons which can be used to improve the organisation's development process. In order to facilitate control, the PIR should have terms of reference, authorised by the approving authority, defining the:-

- scope and objectives of the review;
- criteria to be employed in measuring the achievement of objectives;
- management and organisation of the review team;
- review budget and reporting deadline

3.41 The auditor should evaluate the PIR report to determine the adequacy of efforts in assessing the system.

(Appendix 3.3[29] is a sample Audit Programme that could be considered to perform the System Development Audit)

[29] Adopted from the ICT Audit Guidelines of the National Audit Department of Malaysia (2001)

PART 4 COMPUTER ASSISTED AUDIT TECHNIQUES AND TOOLS (CAATTs)

INTRODUCTION

4.1 Computer Assisted Audit Techniques And Tools (CAATTs), are computer-based tools and techniques which permit auditors to increase their productivity as well that of the audit function in gathering audit evidence by exploiting the power and speed of computer. CAATTs have the ability to improve the range and quality of audit and fraud investigation results. It has nowadays become an integral part of the whole audit work.

4.2 CAATTs may also provide effective tests of control and substantive procedures where there are no input documents or a visible audit trail, or where population and sample sizes are very large. This is done by making use of the wide range of techniques and tools to automate the test procedures for evaluating controls, obtaining evidence and data analysis. The auditor can use CAATTs as an integral part of the whole audit work to gather audit evidence independently. CAATTs provide a means to gain access and to analyze data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system.

OBJECTIVES

4.3 The overall objectives and scope of an audit do not change when an audit is conducted in an Information Technology environment. The application of auditing procedures may, however, require the auditor to consider techniques known as Computer Assisted Audit Techniques (CAATTs) that use the computer as an audit tool.

4.4 CAATTs may be used in performing various auditing procedures and improving the effectiveness and efficiency of obtaining and evaluating audit evidence. CAATTs are often an efficient means of testing a large number of transactions or controls over large population by:

- analysing and selecting samples from a large volume of transaction,
- applying analytical procedures, and
- performing substantive procedures.

4.5 CAATTs make remote and continuous auditing possible. By installing file interrogation tools at remote locations, auditors could continuously monitor activities and report any exceptions to the home office.

4.6 CAATTs may be used in performing various auditing procedures, including the following:

- tests of details of transactions and balances, for example, the use of audit software for recalculating interest or the extraction of invoices over a certain value from computer records.

- analytical review procedures, for example, to identify inconsistencies or significant fluctuations.
- use of expert system, for example, in the design of audit programs and in audit planning and risk assessment.
- tests of general controls, for example, to test the set up of configuration of the operating system or access procedures to the program libraries.
- sampling programs to extract data for audit testing.
- tests of application controls, for example, to test the function of programmed control.
- creation of electronic working papers, for example, by downloading the general ledger for audit testing.
- recommitting calculations performed by the entity's accounting systems.

MAJOR STEPS IN USING CAATTs

4.7 The major steps to be undertaken by the auditor in the usage of CAATTs are to:

- set the objectives of the CAATTs application;
- determine the content and accessibility of the entity's files and data,
- identify the specific files or databases to be examined;
- understand the relationship between the data tables where a database is to be examined;
- define the specific tests or procedures and related transactions and balances affected;
- define the output requirements;
- arrangement with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made with the appropriate cut off data as per the period of audit and time;
- identify the personnel who may participate in the design and application of the CAATTs;
- refine the estimates of costs and benefits;
- ensure that the use of the CAATTs is properly controlled and documented;
- arrange the administrative activities, including the necessary skills and computer facilities;
- reconcile data to be used for the CAATTs with the accounting records.
- execute the CAATTs application;
- evaluate the results.

TYPES OF CAATTS

4.8 CAATTs can be split into two discreet areas of operation namely to validate programmes/systems (*functionality of the programmable controls)* and to analyse data files. Discussed below are some CAATTs that fall in this category.

CAATTs Used to Validate Programmes/Systems

Program Code Review

4.9 Program review involves a detailed examination of programme coding. It generally involves a fair degree of programming skill and a thorough knowledge of programme specification. By reading programme source codes, auditors should identify any of the following[30]:

- *Identify Erroneous Code*: The use of code review to identify erroneous code is well established. Thus auditors can use code review to determine whether program code complies with its specifications.

- *Identify Unauthorised Code*: Without directly examining a program's source code, auditors are unlikely to identify unauthorised code in a program. Unauthorised code often is triggered by a specific data value or combination od data values. For example, a fraudulent programmer might modify a program so it does not print out details of his or her own account when it is overdrawn. Similarly, he or she might modify a program to execlude transactions having certain account number and data values from normal data validation process. Unless auditors submit test data having these specific values and have a way of checking that the test data has travversed all execution paths in the code that is their focus, they are unlikely to detect this unauthorized code.

- *Identify Ineffective Code*: Auditors can examine whether code is ineffictive in two ways. First, they can evaluate whether the code meets the documented program specifications. Second, they can examine wether the code meets user reqirements. Moreover, assuming the program specifications are corect, design errors that results in the program not complying with specification are also prevalent.

- *Identify Inefficient Code*: Code review also can allow auditors to identify inefficient segments of code. For example, in a sequence of tests of transaction types, the tests might not have been ordered according to their frequency of occurrence. As a resulit, the program executes more of its code than it would have to if the tests were recorded. Auditors might also use code review to identify the existance of the instructions that execute inefficiently on the hardware/software platform used.

- *Identify Non-Standard Code*: Non-standard code takes a variety of forms. For example, it could be code that does not comply with organisational standards covering data item names or internal dicumentation. Alternatively, it could be code that does not employ structured programmming control structures. Whatever the nature of the nonstandard code, often it manifests other defects in the code – for example, unauthorised code or erroneous code.

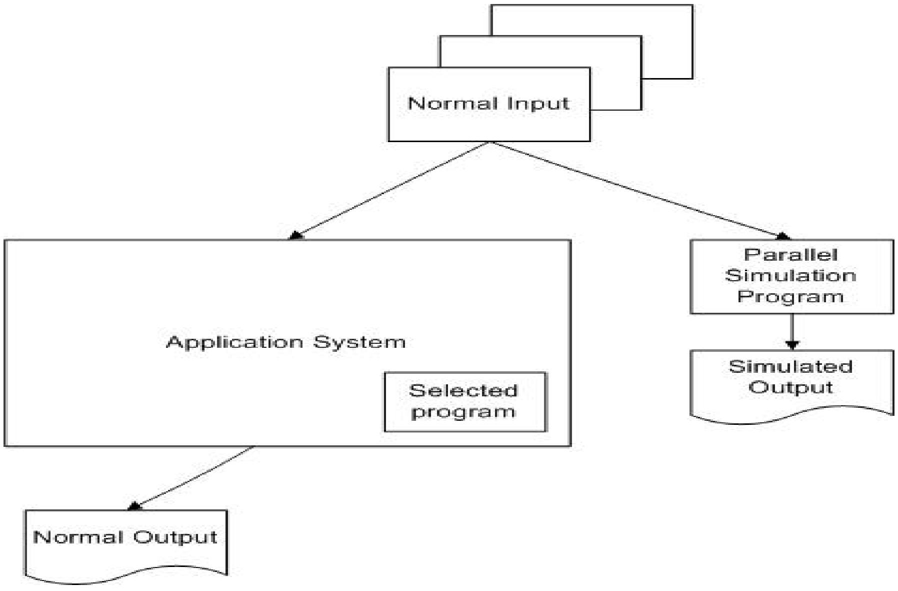
[30] Weber, R. Information System Control and Audit, Prentice-Hall, 1999

Program Code Comparison

4.10 This procedure involves the auditor comparing two versions of the source or object code of the program; one version - called the "blue print" - has known attributes and the auditor determines whether the other version has the same attributes. The auditor uses this technique for two reasons: First, to check whether the software given to him for audit is same as the one in operation; Second, to check whether any changes have been made in the code with respect to earlier versions, and if so, whether adequate change management procedures were followed. Utility programs are available that will compare two versions of a program, and report diffierence between the two.

Parallel Simulation

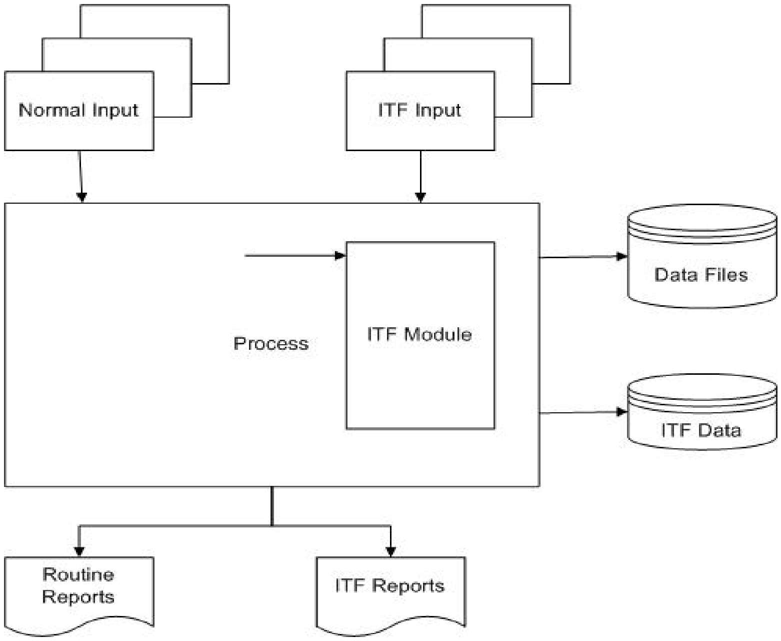
4.11 Parallel simulation involves the creation of an independent set of code that emulates the function of the area being tested. The results can be compared to those produced by the application itself. Parallel simulation is a useful tool enabling the auditor to re-perform all or part of the application being tested. Usually this would be performed on the area of the application of audit interest. This is a good way to prove the accuracy of calculations and processing procedures within the system without affecting the system itself. The auditor will need a good knowledge of the system and of the procedures to be replicated, and programming experience.



PARALLEL SIMULATION

Integrated Test Facility

4.12 An Integrated Test Facility (ITF) is a technique that is sometimes used in auditing complex application systems. It provides an in-built testing facility through the creation of a dummy department or branch within the normal accounting system. Banks sometimes create a test branch within their Customer Accounting System that is used both for audit testing and training tellers in the use of the terminal system.



INTERACTIVE TESTING FACILITY

Tracing

4.13 A trace allows the auditor to analyse each step of a program. By performing a trace it is possible to see how each line of code has an effect on any data being processed or the program itself. For example, if a program is not totalling transactions correctly, a trace can highlight where exactly the error is occurring.

Snapshot

4.14 A snapshot is a utility which allowed the auditor to freeze a program at a given point and give the auditor a view of data at a particular point within a program or system. It is then possible to check on the values of a transaction and the processing that has been going on as the program was running. The snapshot is quick and relatively easy to use although it has a limited function and is specific. This is very useful for identifying potential errors in the mathematical calculations being carried out on a transaction. A good example of a snapshot would be a line of code in a program that produced a halt and output the value of a particular variable.

CAATTs Used to Analyse Data Files

4.15 These are CAATTs which are primarily used on data files. Of course, results of data analysis can indirectly help the auditor to reach conclusions regarding the quality of programs. However, these CAATTs do not directly test validity of programs unlike those discussed earlier.

File Interrogation Software

4.16 File interrogation involves various tests performed on a data file such as to check control totals, duplicate entries, missing entries, abnormal transactions, select samples, etc. The tests can be performed by using SQL statements, writing programmes specific to the system being audited, or by using generalised audit software. Discussed below are two types of file interrogation software.

Generalised Audit Software

4.17 The auditor may face a problem to deal with systems having diverse characteristics: different hardware and software environments, different data structures, different record formats, and different processing functions. With resource constraints it is often not feasible to develop specific programs for every system that will extract, manipulate and report data required for audit purposes. For this reason generalised audit software has been developed that is capable of handling a wide variety of different systems. With the development and marketing of generalized audit software like ACL[31] and IDEA[32], the auditor has been provided with a powerful tool that can add tremendously to the auditor's efficiency with minimum IT-skill requirement.

4.18 The various analytical techniques that can be employed over data using generalized audit software for audit conclusion are:

- Reasonableness and Completeness tests
- Gap and duplication tests
- Period over period and similar comparisons
- Regression analysis
- Statistical analysis
- Transaction matching
- Data mining

Specialised Audit Software

4.19 Some types of audit software packages are now available that are oriented toward a specific industry in which an auditor works. They differ from the generalised audit software discussed earlier in two ways.

4.20 First, since they are oriented toward a particular industry, they provide high-level commands that invoke common audit functions needed within the industry. For example, in the banking industry, they might use a single command to invoke logic that would check for account kiting. If generalised audit software were used to check for kiting, several commands might be required to express the logic needed for various tests.

4.21 Second, industry-specific audit software may run on a smaller number of hardware/software configurations than generalised audit software. Indeed, industry-specific audit software may have been developed to access the data maintained by a *specific* generalised application package that is in widespread use within the industry. Accordingly, the file definitions, record definitions, and field definitions used by the application package may be incorporated in the audit software package, and so do not have to be defined by the auditor each time the audit software package is run.

Embedded Audit Module

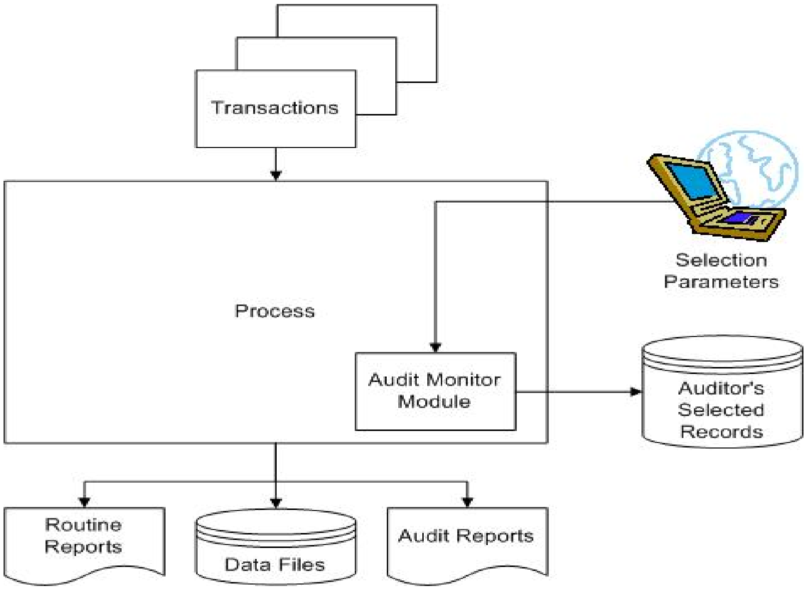
4.22 An embedded audit module is a technique that is generally used with a computer system that handles very high volumes of data. As its name implies, it's an audit application that is permanently resident within the main processing system. The

[31] the website: http://www.acl.com

[32] the website:http://www.audimation.com

embedded audit module examines each transaction as it enters the system. Every time a transaction occurs that meets the selection criteria, transaction details are logged before the transaction is allowed to continue for further processing. The audit log is periodically scanned, analyzed and reports are printed for follow up.[33]

4.23 With embedded audit software, the IT Auditor should be involved in system design and the techniques will have to be developed and maintained within the organisation's application programs/systems.



EMBEDDED AUDIT MODULE

CATEGORIES OF CAATTS

File Downloading Tools

4.24 Using microcomputer-based package, auditors must first receive the data from the host system before it can be processed. There are many methods of data transfer available:

- Small files can be copied directly from floppy disk to the hard disk of the auditor's PC. Larger file may be compressed using a utility such as WINZIP before transfer and decompressed after transfer;
- Data can be downloaded from a reel tape, and most tape readers will be able to access the data;
- Data can be transferred from PC to PC via a parallel or serial cable;
- Data can be downloaded across a network, and its speed is high;
- Data can be downloaded via a modem, although the transfer rate is not very fast, it is also acceptable for smaller files.

[33] Principles of Computer Assisted Audit Techniques—Student Notes , INTOSAI EDP COMMITTEE

4.25 The method used to transfer data depends on the hardware used by the auditor and the auditee.

4.26 File downloading tools are usually used by the CAATTs specialists to transfer clients' data to the auditor's PC. It is carried out by the use of tape management tools, such as Depot, Tarsus, Fdump and Tapeuti. etc

4.27 Auditor also can use Online Database Connectivity (ODBC) to access windows file. The CAATTs user can specify the particular source of data for interrogation from within the file interrogation software and invoke the relevant ODBC driver for that source. In this way direct access between the file interrogation software and the data source can be maintained.

4.28 Sometimes data needs to be manipulated after download, and then it can be put into a format that can be easily be imported into an interrogation package. There are several ways to manipulate data:

- Data can be manipulated using a simple editor such as DOS Text Editor;
- There is a range of Off-the-shelf software to manipulate downloaded data. For example, print files can be manipulated using Auto Import or Monarch. Software Bridge enables the user to translate files from one format to another.
- It is also common to write file manipulation software in house to fix downloaded data. This could take the form of removing padding characters from downloaded data blocks or splitting a downloaded file into small sub files containing different record types.

4.29 File Interrogation Software is the most widely used, and auditor can use it to deal with the massive volumes of data involved. This kind of software usually provides for a wide variety of functions for collecting and analyzing audit evidence, such as:

- Selecting records that confirm to particular criteria;
- Printing selected records for detailed examination;
- Printing totals and subtotals from an accounting file;
- Searching for duplicate transactions;
- Searching for gaps in sequence;
- Comparing the contents of two files, and printing either record matches or exceptions;
- Sorting and merging files in preparation for other audit tests.
- Aging

4.30 *Report Generators Tools*: Such tools facility querying and formatting data in a desired format from a file.

4.31 *System Security/Review Tools*: Software that can help an auditor plan a system review and provide computer generated recommendations, for instance, Enterprise Security Management Software.

4.32 *Planning Tools*: Software that can aid the auditor in planning the auditing.

4.33 *Programming Tools for Specific Tasks (Bespoke Programme)*: Tools usually written by CAATTs specialists to perform a specific function.

Structured Query Language (SQL)

4.34 Structured Query Language (SQL) is the standard language designed to extract data from relational database systems and includes the capability of manipulating both the structure of a database and its data. An SQL interface can be found in database management systems such as Microsoft Query, Microsoft Access, ORACLE, INFOMIX, DB2, INGRES, Dbase IV, etc. SQL is able to perform many mathematical functions: counting, totalling, averaging, multiplication. SQL is also able to generate complex reports using a wide range of conditions: where, between, having, like.[34]

ILLUSTRATIONS ON THE USAGE OF CAATTS

4.35 The following audit steps can be performed by auditor using CAATTs while auditing different areas of operation:

Computerised Inventory Systems

- Identification of items below the standard margins
- Verification of price compliance
- Reconciliation of unmatched pay and remittances to freight invoices
- Identification of negative receipt quantities
- Identification of duplicate items or serial numbers
- Identification of surplus or obsolete inventory
- High value items' analysis
- Determining reorder levels of different quantities by warehouse
- Compute difference between actual and standard costs
- Stock turnover analysis by item (aging)
- Selection of stock sample for reconciliation
- Reconciliation of physical stock levels to computed amounts
- Test for duplicate item numbers, parts or descriptions
- Reporting on products in descending order of profitability

Payroll Applications

- Identification of changes in exemption, gross pay, rates and salary amounts
- Reporting of entries against authorization records for new or terminated employees
- Identify duplicate direct deposit numbers
- Compare pay rates with ranges for the employees' classification
- Identify persons on payroll with no work address, contact numbers, etc.

[34] The National Audit Department of Malaysia, ICT Audit Guidelines, 2001

- Reconcile salaries by job or by project etc.
- Match vendor and employee names, addresses, phone numbers, etc.
- Identification of duplicate employee names, addresses, phone numbers, etc.

DATA RELIABILITY

4.36 Where CAATTs are used to extract information for data analysis the auditor should verify the integrity of the information system and IT environment from which the data are extracted. The reliability of the source of the information used provides reassurance on the findings generated. So ensuring the reliability of data is crucially important. Appendix 4.1 shows the relationship of system controls over data testing requirements.

4.37 There are many verification techniques and procedures that can be used by the auditor:

- Interviewing agency personnel associated with the information system;
- Reviewing and examining the related policies, procedures, and documentation;
- Observing the related activities and operations;
- Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations.

4.38 Several measures can be taken to ensure the reliability of data in electronic computer systems. The first step is to use reliable collection methods. This means that data will be legally obtained from reliable sources, preferably ‘primary’ sources rather that ‘secondary’ sources. The next step to consider is the method by which data is ‘captured’ from the source. Staff will need to be trained in techniques designed to optimize accurate input and to ensure a safe working environment. One of the best ways to ensure the accuracy of data is to apply data verification techniques.

4.39 CAATTs can be used to extract sensitive programs/system information and production data that should be kept confidential. The auditors should safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the auditor should consider the level of confidentiality and security required by the organization owning the data and any relevant legislation.

SAMPLING

4.40 Sampling is used when time and cost considerations preclude a total verification of all transaction or event in a predefined population. The population consists of the entire group of items that need to be examined. The subset of population members is called a sample. Sampling is used to infer characteristic about a population, based on the results of examining the characteristics of a sample of the population.

4.41 The two general approaches to audit sampling are statistical and non-statistical sampling:

Statistical Sampling

4.42 An objective method of determining the sample size and selection criteria. With statistical sampling, auditor can quantitatively decide how closely the sample should represent the population (assessing sampling precision), and the number of times in 100 the sample should represent the population (the reality or confidence level). This assessment will be represented as a percentage. The results of a valid statistical sample are mathematically quantifiable.

Non-Statistical Sampling (often referred to as Judgmental Sampling)

4.43 Auditor should use his/her judgment to determine the method of sampling, the numbers of items that will be examined from a population (sample size) and which items to select (sample selection). These decisions are based on subjective judgment as to which items/transactions are the most material and most risky.

4.44 There are two primary methods of sampling used by auditors—attribute sampling and variable sampling.

Attribute Sampling

4.45 Attribute sampling is typically used for compliance testing of controls whereas variable sampling is frequently used for substantive testing where the sampling unit is often monetary. It should be used when the question of "how many" is pertinent and to determine the characteristics or "attributes" of a population. The results are expressed as a percent of the type of event specified. Each observation is mutually exclusive. An example of an attribute that might be tested is approval signatures on computer access request forms. The following steps can be followed in applying an attribute sample test:

- Determine objectives of test.
- Define the deviation conditions.
- Define the population in terms of time period, sampling unit, completeness of population
- Determine the method of selecting the sample.
- Determine the sample size.
- Perform the sampling plan.
- Evaluate the sample results - Investigate deviations for possible fraud and determine overall conclusions

Variables Sampling

4.46 It is used to answer the question "how much" and applied to populations made up of dollars, pounds, days, etc. It can also provide an estimate of an average or total value of a population. The following steps can be taken to successfully perform a variable sampling test:

- Determine Objectives of test.
- Define the population in terms of sampling unit, completeness of population, and individual significant items.
- Determine the methods of selecting the sample.
- Determine the sample size.

- Perform the sampling plan.
- Evaluate the sample results
    - Project error to population
    - Analyse qualitative aspects
    - Investigate exceptions for fraud
    - Reach an overall conclusion
- Document the above.

Stop or Go Sampling

4.47 It helps prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. It is used when auditors believe that relatively few errors will be found in a population.

Discovery Sampling

4.48 It is used when the expected occurrence rate is extremely low. Discovery sampling is frequently of value when fraud, avoidance of internal controls, evasion of regulation or other critical performance and quality control measures are in question.

4.49 The more commonly used sampling selection techniques are briefly described as follows:

- *Random Sampling*: Each item in the population has an equal chance of being included in the sample, for example, by use of random number tables. The most common method of sampling.
- *Systematic Sampling*: entails selecting the first item at random and then selecting every other item in the sample at fixed intervals.
- *Cluster Sampling*: The universe is formed into groups or clusters of items. Then the items within the selected clusters may be sampled or examined in their entirety.
- *Stratified Sampling*: The items in the population are segregated into two or more classes. Each class is then sampled independently. The results for the several classes may be combined to give an overall figure for the universe or may be considered separately, depending on the circumstances of the test.

Sampling Risk

4.50 Sampling risk is the chance that the sample will not be representative of the population it is drawn from. There are two types of sampling risks: false negatives and false positives.

4.51 A false positive error occurs when the auditor believes a control is working or an account balance is correct when in fact the control is not working or the account balance is incorrect.

4.52 A false negative occurs when the auditor believes a control is not working or an account balance is incorrect when in fact the control is working or the account balance is correct.

4.53 In general, auditors are more concerned with false positives because it impacts audit effectiveness and false negatives effects audit efficiency.

Bibliography

1. AuditNet, www.auditnet.org
2. Barker, D., *Fighting Computer Crime*, Wiley Publications, 1998
3. British Standard 7799: IT – *Code of Practice for Information Security Management*, 2001
4. Carnegie Mellon University, *Capability Maturity Model Framework.*
5. Chaplan, J., *Auditing Information Systems*, Wiley Publications, 1998
6. Dayton, D., *IT Audit Handbook*, Prentice Hall, 1997
7. Efraim, T., *Electronic Commerce - A Managerial Perspective,* Prentice Hall, 2002.
8. General Accounting Office (US), *Federal Information Systems Controls Audit Manual*, GAO, 1999
9. Hickman, J. R., *Practical IT Auditing*, Warren, Gorham and Lamont, 2000
10. Information Systems Audit and Control Association (ISACA), CobiT: *Control Objectives for Information and Related Technology*, 3rd Edition, www.isaca.org
11. Institute of Internal Auditors (IIA)**,** www.theiia.org
12. International Federation of Accountants (IFAC), *Auditing Standards*, 2001, www.ifac.org
13. INTOSAI EDP COMMITTEE, *Principles of Computer Assisted Audit Techniques - Student Notes.*
14. INTOSAI Studying Committee on EDP Audit, *Proceedings on 3rd Working Seminar on Performance Auditing in IT Environment*, 2001.
15. INTOSAI, *IT Audit Courseware*, 2001
16. Krist, M. A., *Standard for Auditing Computer Applications*, Auerbach Publications, 1999.
17. Lainhart, J et al, *Computerised Information Systems Audit Manual*, ISACF, 1992.
18. National Audit Department of Malaysia, ICT Audit Guideline, 2001
19. National Audit Office, *Financial Audit Manual (Module T9) - Audit in an IT Environment.*
20. Pressman, K.S., *Software Engineering – A Practitioner's Approach*, Mc-Graw Hill,2002
21. SAI India, *General Principles of IT Auditing*, 2001
22. Warren, D. et al, *Handbook of IT Auditing*, Warren, Gorham and Lamont, 2001
23. Weber, R., *Information Systems Controls and Audit*, Prentice Hall, 1999.
24. Webopaedia, www.pcwebopaedia.com

IT Standards

The Information Systems Audit and Control Association (ISACA) have published a number of standards for IT auditors in different areas. To help IT auditors follow the auditing standards, ISACA have also published auditing guidelines that map directly to the auditing standards. Of the abovementioned guidelines, the following are considered very useful in helping the IT auditor undertake IT audits:

Guideline	Purpose
060.020.020 Application Systems Review	To describe the recommended practices in performing an application systems review.
060.020.060 Effect of Pervasive IS Controls	To provide guidance in evaluating the effectiveness of IS controls within an organisation.
060.020.070 Use of Computer Assisted Audit Techniques (CAATs)	To provide guidance in the use of CAATs which are important tools for IT auditors in performing audits.

The following international standards on auditing (ISAs) and international auditing practice statements (IAPS) developed by the International Federation of Accountants (IFAC) also give IT auditors professional guidance:

Standard/Guideline	Purpose
ISA 400 Risk Assessments and Internal Control	To establish standards and provide guidance on obtaining an understanding of the internal control structure and on audit risk and its components: inherent risk, control risk and detection risk.
ISA 401 Auditing in a Computer Information Systems Environment	To establish standards and provide guidance regarding auditing in a computer information systems environment.
ISA 600 Using the Work of Another Auditor	To establish standards and provide guidance when an auditor, reporting on the financial report of an entity, uses the work of another auditor on the financial information of one of more components included in the financial report of the entity.

Standard/Guideline	**Purpose**
ISA 610: Considering the Work of Internal Auditing	To establish standards and provide guidance to external auditors on obtaining an understanding of the activities of internal auditing and determining its effect on audit risk.
IAPS 1001 IT Environments – Stand-Alone Personal Computers	Describes the effects of stand-alone PCs on the accounting system and related internal controls and on audit procedures.
IAPS 1002 IT Environments – On-Line Computer Systems	Describes the effects of an on-line computer system on the accounting system and related internal controls and on audit procedures.
IAPS 1003 IT Environments – Database Systems	Describes the effects of a database system on the accounting system and related internal controls and on audit procedures.

Other relevant standards for IT auditors include:

Standard/Guideline	**Purpose**
ISO/IEC 17799 Code of Practice for Information Security Management	Gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation.

Appendix 2.1
[*Page 14*]

IT Controls Frameworks

Few of the most well-known Control Assessment Frameworks are as discussed below:

Internal Control-integrated Framework of COSO

The formal name of this report is Internal Control-integrated Framework. It was published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) in September 1992. The official name of the Treadway Commission was the National Commission on Fraudulent Financial Reporting.

As per COSO report, weak internal controls were the primary contributing factor to many fraudulent financial reporting cases. it stressed the importance of the control environment, codes of conduct, audit committee oversight, an active and objective internal audit function, management reports on the effectiveness of internal control, and the need to develop a common definition and framework of internal control.

COSO defines internal control as a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

One of the key aspects of this definition is that internal control can provide only reasonable, but not absolute, assurance as to the achievement of the objectives. The report further state that each of the above internal control objectives consists of the following five interrelated components, which are derived from the way management runs a business:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

COSO further states that management is responsible for an entity's internal control system, and the CEO should assume ownership of the control system. As per COSO:

- There is a direct relationship between objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives.
- Internal control is relevant to an entire enterprise, or to any of its units or activities.
- Information is needed for all three objectives categories: to effectively manage business operations, prepare financial statements reliably and determine compliance.

- All five components are applicable and important to achievement of operations objectives.

CoCo

The formal name of this report is Guidance on Control. It was published by the Criteria of Control Board (CoCo) of the Canadian Institute of Chartered Accountants (CICA) in November 1995. CoCo defines control and specifies criteria for effective control. The CoCo control framework is intended to be used by people throughout an organisation to develop, assess, and change control.

CoCo defines control as "those elements of an organisation (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organisation's objectives." It defines three categories of objectives:

- Effectiveness and efficiency of operations;
- Reliability of internal and external reporting;
- Compliance with applicable laws and regulations and internal policies.

Cadbury

The formal name of this report is Internal Control and Financial Reporting. It was published in December 1994 by the Committee of the Financial Aspects of Corporate Governance (Cadbury Committee) of the Institute of Chartered Accountants in England and Wales (ICAEW).

***Cadbury** initially defines internal control as:*
The whole system of controls, financial and otherwise, established in order to provide reasonable assurance of:

- effective and efficient operations
- internal financial control
- compliance with laws and regulations

The internal controls are established in order to provide reasonable assurance of:

- the safeguarding of assets against unauthorised use; and
- the maintenance of proper accounting records and the reliability of financial information used within the business or for publication."

Cadbury requires that the board of directors of every company incorporated in the United Kingdom publish a statement about their system of internal financial control. The statement must, at a minimum, acknowledge the following:

- The directors are responsible for internal financial control
- An explanation that the system can provide only reasonable, not absolute assurance against material misstatement or loss
- A description of key procedures that the directors have established to help ensure effective internal financial control
- Confirmation that the directors have reviewed the effectiveness of the system of internal financial control

It encourages directors to state their opinion on the effectiveness of the system of internal financial control.
The criteria for assessing the effectiveness of internal financial control in Cadbury fall into the following five categories:

- Control environment
- Identification and evaluation of risks and control objectives
- Information and communication
- Control procedures
- Monitoring and corrective action

COBIT 3rd Edition

COBIT, stands for Control Objectives for Information and Related Technology. It was published in 1998 after carrying out revisions in the 2nd edition document by IT Governance institute set up by ISACA

The broad objectives and features are outlined as below:

- COBIT now in third edition helps meet the multiple need of management by bridging the gaps between business risks, control needs and technical issues.
- COBIT is a tool for **IT Governance**. [IT Governance has been defined as a set of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.
- COBIT defines control as "the policies, procedures, practices. and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented, detected and corrected."
- Within the framework, there are seven business information requirements, or criteria: effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability. COBIT goes on to specify that IT resources provide the information needed by business processes. COBIT framework identifies five types of IT resources: people, application systems, technology, facilities, and data.
- COBIT is a technology independent framework.
- Audience: Management, to help them balance risk and control investment in an often unpredictable IT environment. Users, to obtain assurance on the security and controls of IT services provided by internal or third parties. **Auditors**, to substantiate their opinions and/or provide advice to management on internal controls.
- The framework continues with a set of 34 high level control objectives, one for each of the IT Processes, grouped into four domains: Planning and Organisation, Acquisition and Implementation, Delivery and Support, and Monitoring. The structure covers all aspects of information and the technology that supports it. By addressing these 34 processes' high level control objectives, the business process owner can ensure that an adequate

control system is provided for the IT environment. Definitions for the four domains identified for the high level classification are:

  - **Planning and Organizing**: This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision need to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.
  - **Acquisition and Implementation**: To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.
  - **Delivery and Support**: This domain is concerned with the actual delivery of required services, which range form traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.
  - **Monitoring**: All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses managements' oversight of the organisation's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

- In addition, corresponding to each of the 34 high level control objectives is an Audit guideline to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement. These 318 control objectives were developed from 41 IT Security, audit and control standards and best practice resources, worldwide.
- In the management guidelines, COBIT specifically provide Maturity Models for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**, which define the most important management oriented implementation guidelines to achieve control over an within its IT processes; **Key Goal Indicators**, which define measures that tell management – after the fact – whether an IT process has achieved its business requirements; and **Key Performance Indicators**, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

Key Points: Introduction of COBIT in SAIs for IT Auditing?

- COBIT was designed for three audiences: Management, Users and Auditors. Auditors can make use of COBIT in substantiating their opinion to management on IT internal controls and to be proactive business advisors. COBIT can be extremely useful to the auditors by providing criteria for review and examination, and by providing, through the framework, an approach to improve audit efficiency and effectiveness.
- COBIT goes on to provide a generic audit guidelines template to assist in the evaluation and testing of the control objectives, The generic approach is to obtain understanding of the process, evaluate controls, assess compliance, and substantiate the risk of control objectives not being met. The template is applied to each of the 34 processes, with specific audit guidelines detailed within each process.
- As a matter of fact, COBIT can be simultaneously adopted as a framework along with other frameworks e.g. INTOSAI / ASOSAI IT Audit frameworks, etc.
- COBIT is a way of thinking. Successful adoption requires orientation, education, and training.
- COBIT is a framework that can be tailored according to the IT environment of the auditee organisation and risk assessment.
- COBIT is not a collection of IT controls and audit programs. COBIT contains IT control objectives that generally must be addressed by most auditee organisations and audit guidelines that may be used to assess performance against those IT control objectives.
- COBIT is an example of clear policy and good practices for IT control and audit that can be used to guide audits.
- Also COBIT framework can be used for performing risk assessments and to guide the development of individual IT audit plans.
- The IT Audit programs can be tailored to include activities from COBIT audit guidelines.
- Compliance focused audit entities and those with less than warm relations with the auditee organisations may need to depend on a mandate for adoption of the COBIT framework.

Capability Maturity Model

- Capability Maturity Model for Software (SW-CMM) is a framework that describes the key elements of an effective software process. The CMM describes an evolutionary improvement path from ad hoc, immature process to a mature disciplined process.
- This framework was given by Carnegie Mellon University of Pittsburgh, USA and was sponsored by the Department of Defense (DoD) of USA.
- The objective of CMU was to provide a model that is based on actual practices, reflects the best of the state of the practice, reflects the need of the individual performing software process improvement and **software process assessments**, is documented and is publicly available.
- The need for such best practices was felt because of reliance on software intensive systems to perform core missions. CMM is a logical framework for base lining an organisations' current process capabilities (i.e strengths and weaknesses)
- **Definition:** CMM is an ordered collection of practices (processes) for the acquisition, development or maintenance of (software – intensive) systems. It is ordered by Key Process Areas.
- It defines the stages through which organisations evolve as they improve their acquisition and implementation processes. It also identifies key priorities, goals and activities on the road to improving an organisations' capability to do its job. It is intended to be independent of the application domain and any specific technology. It also applies to the acquisition of in-house software development
- **Why focus on process?**

  Everyone realises the importance of having a motivated, quality work force, but … even our finest people can't perform at their best when the process is not understood or operating at its best.
- **Maturity levels**

  A maturity level is a well defined evolutionary plateau on the path to becoming a mature software acquisition / development organisation.

  There are five maturity levels in CMM.

  Maturity levels may not be skipped. Each level is a layer in the foundation for continuous process improvement.
- **Key Process Areas**

  Key Process Areas (KPAs) are a cluster of related practices performed collectively to achieve a set of goals. Each maturity level in CMM is composed of several Key Process Areas.

  They are the major building blocks in establishing the process capability of an organisation.

  Each KPA has been defined to reside at a given maturity level.

  There are 16 KPAs in the CMM(SW).
- CMM can be adopted in IT Auditing for software process assessments, in which a trained team of IT Auditors determine the state of the organisations' current software process and reports the high priority software process related issues facing an organisation.

IFAC Guidelines

IT Committee of the IFAC came out with a series of guidelines to promote executive understanding of the Key issues affecting the management of information and communications. The series of guidelines were released in the year 2002.

The guidelines are published in six parts – (1) Managing Security of Information, (2) Managing IT – Planning for transact, (3) Acquisition of Information Technology, (4) The Implementation of IT solutions, (5) IT service delivery and support, (6) IT Monitoring.

In this series of guidelines, the International Federation of Accountants' IT committee seeks to promote executive understanding of key issues affecting the management of information and communications. Everyone including IT auditors who have a specific role and / or responsibility for achieving IT goals and processes can gain from these concepts.

Apart from the IT guidelines, International Standard on Auditing published by IFAC contains International Auditing Standard 400 for Risk Assessment and Control and International Auditing Standard 401 on Auditing in a Computerised Information System environment. Also International Auditing Practice statements No. 1001, 1002 and 1003 deal with auditing issues related with IT environments for Stand Alone computers, online systems and database systems respectively.

British Standard 7799-1:2000

BS7799 is the British standard for Information Security Management. It has now become an International Standard, ISO 17799. It is in two parts - Part 1 sets out approximately 40 objectives for Information Security, and Part 2 has about 130 controls which can be implemented to achieve those objectives.

It is applicable to every organisation, whatever the type of organisation, and whatever its size. There are a rapidly-growing number of organisations who not only comply with it, but also are independently certified to be complying with it. There are both British and International Users' groups. It provides organisations with a framework of Information Security, which can be recognised by other organisations.

BS7799 is the most widely recognised security standard in the world. Although it was originally published in the mid-nineties, it was the re-vision of May 1999 which really put it on to the world stage. Ultimately, it evolved into BS EN ISO17799 in December 2000.

BS 7799 (ISO17799) is comprehensive in its coverage of security issues, containing a significant number of control requirements. Compliance with it is consequently a far from trivial task, even for the most security conscious of organisations.

SAC Report of Institute of Internal Auditors

The Systems Auditability and Control (SAC) report is intended to provide "sound guidance on control and audit of information systems and technology. The report focuses on the business perspective of information technology and the risks associated with planning, implementing, and using automation." SAC emphasizes management's responsibility to identify, understand, addresses the risks associated with the integration of technology in an organisation, and to oversee and control the organisation’s use of technology. The SAC report was originally published by the IIA in 1977. It was the first internal control framework pertaining to IT, Due to the enormous changes in IT since 1977, an updated and extended SAC report was published in 1991, and was then further revised in 1994.

SAC defines the system of internal control as those processes, functions, activities, subsystems, procedures, and organisation of human resources that provide reasonable assurance that the goals and objectives of the organisation are achieved, and which ensure that risk is reduced to an acceptable leve1.

The SAC report consists of fourteen modules: Executive Summary, Audit and Control Environment, Using Information Technology in Auditing, Managing Computer Resources, Managing Information and Developing Systems, Business Systems, End-User and Departmental Computing, Telecommunications, Security, Contingency Planning, Emerging Technologies, Index, Advanced Technology Supplement, and a case study.

AICPA Statement on Auditing Standards 55 and 78

The AICPA's Statement on Auditing Standards (SAS) 55 and 78 pertain to the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted auditing standards. The SAS 55n8 definition of internal control is identical to that of the COSO report. In addition to the three COSO objectives of internal control (efficiency and effectiveness of operations, accuracy of financial reporting, compliance with applicable laws and regulations), SAS 55/78 also emphasizes the testing of relevant financial reporting and operational controls in order to assess whether the assets of an entity are adequately safeguarded.

As with the other internal control frameworks, SAS 55/78 states that, "Internal control, no matter how well designed and operated, can only provide reasonable assurance to management and the board of directors regarding the achievement of an entity's control objectives."

What are the keys to a successful Control Assessment Program?

The basic keys for making a Control assessment program a successful venture in any organisation is to take care of the following:

- The most important part of any Control assessment program is the need to obtain the encouragement and support of senior management. This is more applicable to internal audit than to external audit. Without their backing, lower levels of management will not be anywhere near as likely to take the process seriously. Without serious participation, a Control assessment program could be viewed as a waste of time.
- The second key to a successful Control assessment program is to ensure senior management support through effective demonstrations of

the potential for significant gains in operational efficiency and effectiveness, and reductions in exposure to financial, regulatory, and other significant risks. These demonstrations can be supported by success stories at various organisations that have implemented successful Control assessment programs. Articles written about Control assessment may need to be referred to, and senior management may have to be better educated on the objectives of internal controls.

- The third key to a successful Control assessment program is proper training of auditors in the skills necessary to facilitate assessment. Till now, auditors have interacted with client staff and management on a one-on-one basis or in small group meetings. Auditors were not typically required to facilitate discussion by other groups. However, as Control assessment becomes more and more the norm in leading-edge companies, the demand for IT auditors as well as non-IT auditors who possess Control assessment facilitation skills will be significantly enhanced.

  Since Control assessment is a relatively new phenomenon, there are very few auditors on the market today who have Control assessment facilitation skills. As a result, many firms are finding it necessary to send some of their staff to attend facilitation training in order to have their facilitation skills. Because facilitation skills are often used by many course instructors, the training department within an organisation should be able to assist in finding facilitation courses. Other possible sources would be conferences and seminars sponsored by local chapters and international headquarters of internal auditing professional associations such as the IIA and the ISACA.

  Auditors must also be highly knowledgeable about the particular internal control framework(s) adopted by an organisation's audit department. Therefore, training of both IT and non-IT auditors on the details of the applicable internal control framework(s) is also critical.

- A fourth key to Control assessment success is having the proper tools. These tools include a private conference room or training room with flipcharts, marking pens, whiteboards or chalkboards, and other typical training materials, in addition to automated tools such as a laptop computer, etc.

Appendix 2.2
[*Page 16*]

Preliminary Data Gathering Check List

1. Determine Personnel Responsible

Determine the IT staff and primary users responsible for the oversight of IT Application(s) being audited.

2. Technical Information about the Systems

- Determine what hardware is used to run the system,
  - Classify the system as micro, LAN, client/server or mainframe based.
- Determine what operating system is used to control the environment.
- Determine if the software was purchased or developed in-house.
  - When it was developed and what modifications have been made since the initial development?
- If the software was purchased, determine if any vendor warranties are still in force.
- Verify that the software was developed and updated based on a sound "Systems Development" methodology.
- Identify the programming languages used in the application.
  - Determine who is responsible for normal and abnormal maintenance.
  - If responsibility is in-house, determine if the IT department has programming staff knowledgeable in these programming languages.
- Determine whether the system processes data on-line, by batch or in combination.
  - Identify the types of data files used in processing (database, sequential files, disk tape).
- Identify the primary transaction, master and reference files used in processing and where they come from (data entry, automatic transfer, etc.).
- Determine how the IT department controls and secures access to the application programmes and data.
  - Identify the access facility to control basic sign-on and any others such as database task definitions, file and record restrictions, etc.
- Browse the programmers' Application Documentation (This should include system and program flowcharts, decision tables, file layouts, data element definitions narratives, source program listing, and record of changes. The documentation should also indicate on which platform the various portions of the system operate).
- Browse and evaluate the quality of the application operations documentation. (This should include job and system flowcharts, input and output descriptions, job frequency and sequence of operation, job restart / recovery procedures, file backup requirements and procedures, error messages and reconciliation techniques, report distribution procedures, data capture instructions).
- Determine if backup copies of application program and operations documentation are stored off-site.
- Determine if the IT department monitors processing flows to verify application program run according to schedule.

3. End User Computing Information

- Interview a sample of end-user managers to determine end-user management attitudes regarding the quality and effectiveness of the system.
- Determine from end-user management what they perceive to be the risks, exposures and limitations associated with the system.
- Determine the number of end-users working with the system, their locations and responsibilities associated with the system.
    - Obtain an organisation chart for these positions and people.
- Determine if this application generates data for legal or regulatory agencies.
- Evaluate the quality of end-user documentation (This should include description of the system, description of source documents and procedures for their preparation, job submission procedures, control procedures, error identification and correction procedures, description of output reports and their use).
- Identify the application training available for end-users.
    - Evaluate this training to determine if it is adequate, current and available for new people.
    - Determine how much training has actually been provided.
- Determine if end-user activity is adequately supervised.

4. Information about System Interfaces

- Are there interfaces of the Application being audited with other applications. If yes, then what is received from and what is sent to these other applications.
- Determine how end users verify or assure that the interfaces are providing complete, accurate, and authorised data.

5. Information about File Handling

- Determine the retention periods for the various key application data files.
    - Evaluate if the retention periods satisfy management reporting, and other legal and internal accounting requirements.
- Determine if management and data owners are aware of the retention periods of the various key application data files, and if these managers are satisfied with the length of retention. Determine whether actual retention is consistent with requirements.

6. Backup and Recovery Procedures

- Identify the key system files
    - Determine how often key files are backed up.
    - Determine if copies of these backup files are stored at a suitable off-site location.
- Assess whether that the off-site backup files storage facilities are secure.
- Determine if application recovery plans exist (both technical and end-user) for restoring from short-term and long-term interruption of computer processing.
    - Verify whether these plans address both technical restoration needs and alternative end-user processing procedures.
- Determine if these application recovery plans have been tested regularly.

- Establish how long the organisation could comfortably function and avoid significant financial loss if the computerised aspects of this application failed.
  - Verify that restart/recovery and disaster recovery plans provide for restoring this application the time needed to avoid significant financial loss.
  - Evaluate alternate plans of the management, should the application not be able to be restored in time.
- Determine if the IT department has established data file and record retention periods.
  - Determine if these retention periods are reasonable for backup, disaster/recovery and audit purposes.
- Verify that restart/recovery plans from short-term computer interruptions include the ability to identify the status of all processing to the point of application failure to establish a cutoff for transaction re-entry.

7. Identify all Sub-systems

- Identify all subsystems associated with this application and the objectives of each sub-system.

8. Information about Data Input

- Determine whether data entry procedures and controls are effective to ensure complete and accurate input of data.
- Determine that online edit routines identify inaccurate data as early as possible and prevent the entry of invalid / duplicate / out of period data into the system.
- Determine that invalid data is properly rejected during subsequent processing of data input.
- Review transactions and determine that the screens are effective and useful.
- Determine that controls over correcting errors are effective and that errors are corrected and resubmitted on a timely basis. Identify any cost beneficial improvements in error correction procedures.

9. Processing Information

- Determine that job documentation is accurate and effective for proper scheduling and restart/recovery.
- Review user and IT data control procedure relating to job scheduling to ensure that jobs are run in the correct sequence, and that no data is inappropriately added, changed or lost during processing.
- Review the IT problem reports to identify problems relating to the application system.
- Determine that end user problems are identified and resolved on timely basis.
- Determine if any significant problems are not reflected on the problem reports and follow up as required.

10. Information about Output

- Review output distribution to determine that output is distributed on a timely basis only to authorised personnel and that restricted output is properly labeled.
- Review user balancing and reconciliation procedures to ensure that out of balance conditions are resolved on a timely basis.
- Reviews reports generated with users and determine their necessity and usefulness.
- Determine if any reports could be eliminated or if any additional reports could be beneficial.
- Determine that reports are retained for proper periods of time.

11. Change Management Information

- Determine program change requests are documented in writing that users assist in developing test data, review test results, and approve all program changes in writing prior to being placed into production.
- Review controls over changes to user developed programs (if these programs perform significant processing).

Appendix 2.3
[*Page 16*]

Survey Questionnaire For IT Applications

Form 1

1. Name of the auditee organisation: Date of sending the data:_____________
____
____

2. Name of the IT Application and broad functional areas covered by the IT Application:
____
____
____
____
____
____
____
____

		Name	Phone No.	Email
3.	Department Head of the auditee organisation	________________	______________	_________
4.	Information Systems In-charge	________________	______________	_________

5. What is (are) the location(s) of the IT system installation(s)?
____
____

6. State the category of IT system architecture:

A. Mainframe based □
Minicomputer based □
PC based □

B. File server system □
Client server system □
Distributed processing system □
Web based/EDI □

7. State the category of IT application. (Please indicate the choice(s) applicable):

Accounting system □
Financial management system □
Inventory/Stock Management □
Decision support system/MIS □
Manufacturing/Engineering □
Payroll □
Personnel and Administration □
Marketing □
Sales □
ERP □
R&D □
Others (Please specify) □

____

Whether the above IT application has got a bearing on the financial and accounting aspects of the organisation?

Yes □ No □

8. Software used (the Version may also be specified):

Operating system(s) __________________________
Network software __________________________
Communication Software __________________________
DBMS / RDBMS __________________________
Front end tool __________________________
Programming Language(s) __________________________
Bespoke (Vendor developed) __________________________
Utility Software __________________________
Any other __________________________
____

9. Is the IT system a mission critical system or an essential system?

Mission critical system[β] □
Essential system[γ] □

10. Has the application system been/being developed in house or by outsourcing?

In house □ Outsource □

[β] A mission critical system is an IT system which directly impact the primary function of the organisation e.g. Passenger Reservation System in Indian Railways.

[γ] An essential system is an IT system the loss of which cause disruption of some service without disrupting primary services.

In case of outsourcing, specify the name of agency and the contracted amount:

____

____

(P.S. – If the IT system is still under development, rest of the information in questionnaire from Sl. No. 11 to 18 may not be furnished. In that case Form 3 may be filled and if procurement of H/W for IT system under development has been done, then Form 2 may also be filled.)

MM YY

11. When was the system made operational? ____________________________

12. What is the total investment on the IT system project? Indicate the investment in terms of millions of monetary unit of currency applicable[α]:

Hardware items ____________________
Proprietary software ____________________
Application System development cost ____________________
Manpower training cost ____________________
Maintenance of the all components (recurring) ____________________

13. Number of persons engaged for operation of the system?

1 – 10 □
11 – 25 □
26 – 50 □
51 – 100 □
> 100 □

14. What is the average volume of transactional data generated on a monthly basis in terms of storage space?

____

15. Does the system documentation provide for an audit trail of all transaction processed and maintained?

Yes □ No □

16. Are the manuals as indicated available?

a. Users documentation manual Yes □ No □

b. Systems and programming documentation manual Yes □ No □

[α] If exact figures are not readily available, approximate figures may be provided.

17. Is there any system in place to make modifications to the application being used on a regular basis to support the function?

Yes □ No □

18. Does the organisation transmit/receive data to/from other organisations?
Receive □ Transmit □ No □

Form 2

19. Details of all Hardware items including the number of terminals etc. employed:

____

____

____

____

____

20. Details of networking hardware employed:

____

____

____

____

21. Are more than one IT Application(s) running on the same Hardware? If Yes, specify the name(s) of such IT Application(s) apart from the application as indicated at Sl. No. 2.

____

____

____

____

Form 3

22. What is the current status of development of IT system if it is still under development? (Tick the appropriate box indicating the current stage of development of IT Application)

Feasibility study stage □

User requirement
Specification stage □

Design stage □

Development stage □

Testing stage □

Parallel run (if any) □

Implementation stage □

23. What is the projected cost for the IT system?
____

24. What is the target date for completion?
________________(MM/YY)

Appendix 2.4
[*Page 17*]

General IT Controls: A Sample Audit Programme

Perform a General Controls review of Information Technology (IT). The reviews will include all IT related policies, procedures, data security administration, data center operations, system development / maintenance, the IT Disaster / Recovery plan and its relation to the corporate Business Continuity plan.

Audit Steps	**Yes**	**No**	**Remark**
IT General Controls			
Planning			
Determine if committees review, approve, and report to the board on: Short and long term information systems plans IT operating standards Data security policies and procedures Resource allocation (major hardware/software acquisition and project priorities) Status of major projects IT budgets and current operating cost			
Policies, Standards, and Procedures			
Determine whether the board of directors has reviewed and approved IT's policies.			
Examine how IT management has defined standards and adopted a methodology governing the process of developing, acquiring, implementing, and maintaining information systems and related technology. Determine if IT management has adequate standards and procedures for: Systems development Program change control Data Center operations Data Base administration Performance monitoring Capacity planning Network administration Information security Contingency planning/disaster recovery			
Assess compliance with these policies and procedures.			
Data Security Administration and Accountability			
Verify the names associated with the DBA function.			

Determine that the DBA is prohibited from routine operating duties in the computer facility. (this person should not have system operating duties and should be sufficiently independent from the computer operation to ensure that he/she cannot create, delete, or suppress passwords in order to cover improper activities.)			
Security Policy			
Review the data security policy. Determine if the security procedures cover: Physical protection of the facility. Designation and duties of the security officer(s). Authorised data and program access levels. Requirements for password creation and change procedures. Requirements for access via terminals, modems or computer system (LAN) connection. Monitoring and follow-up of security violations. Determine whether procedures are in place to update the security policy. Ensure updates to the policy and procedures are distributed to and reviewed by management. Determine if an education program has been implemented to promote user awareness about security policies and procedures.			
Data and Program Security			
Determine how access levels are granted. Whether all access is restricted unless specifically authorised. If the password file is controlled (e.g., encryption). How security violations are detected and reported. Determine that password security is in effect on all applications. Assess the adequacy of controls over: Development and test programs. Identify whether levels of access are periodically reviewed. Assess whether passwords, user IDs are adequately controlled for: Changing on a regular basis Suppressing passwords on a terminal. Determine that passwords are removed as soon as an individual's employment is terminated to ensure that a terminated employee cannot gain access to the computer files through an outside terminal.			
Security Controls			
Obtain copies of the security access and control files for the operating system. Obtain a list of data altering utilities, user exits, user interface programs, and privileged commands. Using these documents,			

determine: Whether the data security administration function is independent of systems and programming. If all programmers have unique user IDs and passwords. If system access levels are consistent with job functions. If all changes to the system security software are approved by the system security administrator. If security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed and the nature of the access. The adequacy of segregation of duties for application programming, systems programming, computer operation, and system security functions. If physical or logical separation between the production and test environments is maintained. The adequacy of controls over dial-up access.			
IT Servicing			
Provider			
Obtain a list of services performed by the data processing center. Determine if written contracts are in effect for all customers. Review a copy of the contract(s) used.			
Receiver			
If receives major support from one or more outside service provider(s): List the name(s) and location(s) of the service provider(s). Prepare a listing of the services outside vendors provide. Assess the adequacy of the procedure for monitoring the financial condition of its service provider(s) and whether the procedure is sufficient to project the continued viability of contracted services.			
Insurance			
Review the adequacy of insurance coverage (if applicable) for: Employee fidelity (blanket-bond) IT equipment and facilities Loss resulting from business interruptions Determine whether the board of directors has approved requirements for related insurance coverage. Examine the business-interruption coverage limits.			
Recovery Planning			
Determine if IT has a documented disaster recovery plan. Verify that the IT disaster recovery plan supports the goals and priorities found in the corporate business continuity plan.			

Review the IT disaster recovery plan to determine if it: Clearly identifies the management individuals who have authority to declare a disaster. Clearly defines responsibilities for designated teams or staff members. Explains actions to be taken in specific emergency situations. Allows for remote storage of emergency procedures manuals. Defines the conditions under which the backup site would be used. Has procedures in place for notifying the backup site. Has procedures for notifying employees. Establishes processing priorities to be followed. Provides for reserve supplies. Determine if all critical resources are covered by the plan. Determine if a copy of the IT contingency plan is stored off-site. Determine if the backup site: Has the ability to process the required volume. Provides sufficient processing time for the anticipated workload based on emergency priorities. Allows the subsidiary to use the facility until it achieves a full recovery from any interruption. Determine if there is physical security at the recovery site. Determine what agreements, commitments, or projections have been made with and by hardware vendors regarding the period of time required to replace hardware. Verify that vendors has been identified. Determine if: Duplicates of the operating system are available on and off site. Duplicates of the production programs are available on and off site (including both source and executable versions). Determine if all master files and transaction files are backed up adequately to facilitate recovery. Determine if the IT disaster recovery plan is tested at least annually, including critical applications and services Determine if the tests include: Setting goals in advance. Realistic conditions and activity volumes. Use of actual backup system and data files from off-site storage. Participation and review by internal audit. A post-test analysis report and review process that includes a comparison of test results to the original goals.			

Development of a corrective action plan for all problems encountered. Determine if several user departments have been involved in testing at the same time to uncover potential conflicts.			
SYSTEMS DEVELOPMENT AND PROGRAMMING			
Project Management and Control			
Determine whether there is a written plan for future changes to current hardware, software, or the addition of new applications. Obtain a copy of the plan and note major items.			
Standards			
Determine whether policies and procedures are adequate for: Application systems / program development Operating system maintenance Program change control Testing Program and system documentation Implementation			
Application Systems Development			
Obtain a list of all application systems currently in use or under development. Indicate if the applications were purchased or developed in-house. Determine whether: All required documentation is present and sufficiently detailed to evidence complete compliance with established standards. The structure of the System Development Life Cycle (SDLC) planning includes all appropriate phases and whether they were completed as prescribed by the plan. The audit trails, exception reports and system security designs are adequate. User manuals are adequate. The board, senior management, applicable committees, computer operations, user departments, and audit were involved in all phases of the development process. For purchased software: Determine whether new releases are tested before installation. Determine if the most recent release is being used. Application Program Development Review selected documentation for at least one in-house developed program. Trace the program's development from the initial request through the post implementation review process. Determine: If all required documentation is present and sufficiently detailed to evidence compliance with established programming			

procedures. Whether the program meets the objectives of the original request, based on test results and user feedback. For program requests, determine: Whether program request procedures were followed. If a user department was affected, whether there was appropriate consultation between users and the IT department. Whether appropriate documentation and training was provided to users and computer operators.			
Operating System Maintenance			
Obtain and review the operating system installation plan, the system generation report, the system log, and other system related activity reports. Review changes made to the operating system and supporting system software to determine compliance with procedures. Determine if: The overall supervision by management over system programmer activities is adequate. Controls over the following are adequate: New system installation Implementation of new releases In-house enhancements Emergency fixes and other temporary modifications Documentation of changes System testing Management or supervisory approvals.			
Program Maintenance			
Review program changes to determine compliance with procedures and the adequacy of internal control. Determine: If the program change control procedures provide adequate guidelines to control the function. If change standards and procedures are adhered to. If documentation is complete. The adequacy of involvement of users, audit, and IT management in the request and approval processes. For emergency program fixes and other temporary changes, determine if: Prescribed procedures are followed. Documentation is sufficiently detailed to explain the nature of the emergency change, the immediate action taken to address the problem, and subsequent actions to permanently correct the problem.			

Testing			
Determine whether procedures require that: The scope of testing includes all functions, programs, and interface systems. All test discrepancies are adequately documented and resolved. Users participate in the actual testing phase All test plans and results are documented and retained			
Documentation			
Determine if: Overall systems and program documentation adheres to standards. Documentation is complete and current.			
Implementation			
Review documentation generated from the implementation process and determine if: Controls ensure complete integrity of programs between the test and the production environments. System level implementations are subject to the same controls as application level activity.			
Vendor Software/Support			
Obtain and review copies of all vendor and consultant contracts, available financial statements and escrow agreements. Ensure software purchase and selection procedures require: Clear definition of user requirements Clear definition of system requirements (equipment, interface, etc.) Cost/benefit analysis. Software support (in-house or vendor provided) Financial condition of vendor. Escrow agreements. User documentation and training.			

Appendix 2.5

[*Page 22*]

Evaluation of Organisational and Management Controls: A Sample Audit Programme

OVERALL POLICY, MANAGEMENT AND CONTROL	**Yes**	**No**	**Remark**
1 IT Strategy How appropriate is the audited body's IT strategy? • Has it been approved? • Is it kept up to date? • Does it cover the financial information systems? • Are staff informed of the issues? • Are there procedures for monitoring its implementation? *A poor or absent IT strategy could lead to the development of systems which are unsuitable for business needs. An IT strategy can help the auditor identify new systems at an early stage.*			
2 Senior Management Involvement How does senior management maintain an appropriate level of interest in the audited body's IT functions? (E.g. IT steering committees.) *Management disinterest may lead to uncontrolled systems development and unauditable systems. Senior management can also provide impetus to the development and operation of other computer controls.*			

	Yes	No	Remark
3 Documentation Policies Does the client have adequate IT documentation policies? Policies should ensure that documentation is up to date, comprehensive and available to appropriate staff. *Inadequate documentation policies increase the risk of unauthorised working practices being adopted, and may render the system difficult to maintain.*			
4 Record/Document Retention Are there appropriate policies for retaining electronic documents and computer prints? E.g. • Electronic records • Old Trial Balances • Capacity planning *The lack of such policies could result in difficulty in obtaining audit evidence, e.g. if records are deleted or archived.*			
5 Internal Audit Involvement Does the organisation's internal audit function carry out IT reviews of the computerised financial systems? • What are its remit and scope? • IT skills/training/experience *It may be possible to place reliance on the work of internal audit. They may be able to identify particular audit risks. The auditor may need to refer to the annual review of IA's work.*			
6 Personnel Policies Are policies appropriate for the IT environment? E.g. high turnover: • recruitment screening • disciplinary policies *Inadequate personnel policies increase the risk of poorly trained staff making mistakes, fraud by unvetted employees and sabotage by disgruntled staff.*			

	Yes	No	Remark
7 Computer Security Policies Is the security police adequate? • Is it based on risk assessment? • Has it been circulated to staff? • Is it kept up to date? • Does it cover the reporting of incidents and security weaknesses? • Is there IT security training? • Who is responsible for security? • What compliance checking is done? *Inadequate security policies may lead to staff and management being unaware of security risks and their responsibilities.*			
8 Legal and Regulatory Issues Does the organisation have appropriate policies and procedures for ensuring that its IT facilities comply with legal and regulatory requirements? *The absence of appropriate policies increases the risks of irregular operations (i.e. failure to comply with legislation or regulations, e.g.* *The Data Protection Act* *Health and Safety Regulations*			
9. Market Testing/Outsourcing/Facilities Management Does the audited body receive IT services from external sources? Have appropriate procedures been developed to meet identified risks (e.g. access rights)? Are there any plans to use third party IT service providers? *The use of independent service providers, both internal and external, can increase the risks to data availability and integrity. Without appropriate controls, it may not be possible to place reliance on the data supplied by the external service suppliers.*			

Appendix 2.6
[*Page 39*]

Evaluation of Input Controls: A Sample Audit Programme

INPUT CONTROLS	**Yes**	**No**	**Remark**
1 What procedures/controls are there to ensure that data input is authorised and accurate? E.g. • Authorised user lists • Standard input forms • Format checks • Range checks • Reasonableness checks • Dependency checks • Use of check digits *Inadequate input controls increase the risk of erroneous or fraudulent data being input for processing.*			
2 What measures have been adopted to prevent the duplicate input of transactions? E.g. • Use of unique reference numbers • Physical cancellation of source documents • Logical rejection of duplicate input *There should be manual and/or computer controls to reduce the risk of duplicate transaction processing.*			

	Yes	**No**	**Remark**
3 How are staff assured that all valid transactions have been input? What controls are there to ensure that all input documents have been received, i.e. completeness and accuracy checks. • Batch totals • Hash totals • Sequence checks Completeness and accuracy controls reduce the risk of incomplete or missing input data.			
4 What procedures are there to deal with rejected transactions? *Inadequate procedures increase the risk of incomplete financial statements.*			
5 What actions are there taken by management to monitor data input? *Management monitoring and review reduces the risk of unauthorised data input. Management review also ensures that established input procedures are being followed.*			
6 Is data required to be converted before input? If so, what measures are taken to ensure that converted data is accurate and complete? *Data transferred from one computer system may have to be converted before it can be input into another. Inadequate conversion controls increase the risk of inaccurate or incomplete transaction data.*			

Appendix 2.7
[*Page 41*]

Evaluation of Processing Controls: A Sample Audit Programme

PROCESSING CONTROLS	Yes	No	Remark
1 What controls are there to ensure that all transactions have been processed? E.g. • Input/output reconciliation • Sequence checking • Control totals *Inadequate controls over processing data increases the risk of incomplete, erroneous or fraudulent transactions being processed.*			
2 What controls are there to ensure that the correct files are processed, e.g. pay-roll runs, weekly runs, etc.? Controls can be physical or logical in nature. E.g. • Disk/tape labels • Use of file headers • Marking of previously run files *Inadequate controls over data files increases the risk of the wrong transaction data being processed.*			

	Yes	**No**	**Remark**
3 How do the application and staff deal with processing errors? Are invalid transactions rejected and operators informed? *Inadequate controls to follow up rejected transactions increases the risk of rejected, but valid transactions being excluded from the financial statements.*			
4 What controls are there to ensure the accuracy of processing? E.g. • Control totals • Range/validity checks • Use of check digits *Inadequate controls increase the risk of undetected and uncorrected processing errors.*			
5 What controls are there to detect/prevent any duplicate processing? *Inadequate controls increase the risk of transactions being processed on two or more occasions.*			

Appendix 2.8
[*Page 42*]

Evaluation of Output Controls: A Sample Audit Programme

OUTPUT CONTROLS	**Yes**	**No**	**Remark**
Are there controls to ensure that computer output (printouts, cheques, invoices, purchase orders, etc.) is stored correctly and that when dispatched they reach their proper designation? *Inadequate controls increase the risk that errors in processing will not be brought to management's attention.*			
Are there appropriate controls over the storage of computer stationery? E.g. • Payable orders • Software license *Inadequate controls increase the risk of fraudulent activity and incomplete accounting records.*			
What reasonableness, accuracy and completeness checks are carried out on output? E.g. sequential page numbering, run to run controls. *These controls are used to detect processing errors and/or unauthorised processing.*			
Are appropriate controls exercised over the production, storage and transportation of tapes and other media? *Do the controls comply with current guidance?* *Inadequate controls increase the risk of unauthorised payments.*			

Appendix 3.1

[*Page 57*]

Excerpts From INTOSAI Auditing Standard On Independence

2.2.25 The SAI must remain independent from audited entities. It should, however, seek to create among audited entities and understanding of its role and function, with a view to maintaining amicable relationships with them. Good relationship can help the SAI to obtain information freely and frankly and to conduct discussions in an atmosphere of mutual respect and understanding. In this spirit, the SAI, while retaining its independence, can agree to be associated with reforms which are planned by the Administration in areas such as public accounts or financial legislation or agree to be consulted about the preparation of draft laws or rules affecting its competence or its authority. In these cases it is not, however, a matter of co-operating with certain administrative services by giving them technical assistance or by putting SAI financial management experience at their disposition.

2.2.26 In contrast to private sector audit, where the auditor's agreed task is specified in an engagement letter, the audited entity is not in a client relationship with the SAI. The SAI has to discharge its mandate freely and impartially, taking management views into consideration in forming audit opinions, conclusions and recommendations, but owing no responsibility to the management of the audited entity for the scope or nature of the audits undertaken.

2.2.27 The SAI should not participate in the management or operations of an audited entity. Audit personnel should not become members of management committees and if audit advice is to be given, it should be conveyed as audit advice or recommendation and acknowledged clearly as such.

2.2.28 Any SAI personnel having close affiliations with the management of an audited entity, such as social, kinship or other relationship conducive to a lessening of objectivity, should not be assigned to audit that entity.

2.2.29 Personnel of the SAI should not become involved in instructing personnel of an audited entity as to their duties. In those instances where the SAI decides to establish a resident office at the audited entity with the purpose of facilitating the ongoing review of its operations, programs and activities, SAI personnel should not engage in any decision making or approval process which is considered the auditee's management responsibility.

Appendix 3.2
[*Page 59*]

System Development Life-Cycle Risks

Objective: To obtain application to specified standards, at reasonable cost, within budget and by deadlines.
Risks are that:-

- application do not meet user needs or requirements;
- application are not available when required or supplier fails to deliver;
- application are not of the required quality;
- application are purchased without adequate authorisation;
- application are purchased at inflated prices;
- government/legal procurement directives/legislation are not observed;
- inadequate business case;
- maintenance arrangements give poor value for money.

Objective: To obtain services from a supplier in accordance with a specified set of terms governing requirements, obligations and remuneration.

Risks include:-

- failure to maintain service levels;
- monopolistic relations develop;
- contracts inadequate for the enforcement of supplier obligations,
- confidentiality of client data;
- inadequate management of the contract;
- escalating cost.

Appendix 3.3
[*Page 66*]

Reviewing System Development: A Sample Audit Programme

A. GENERAL

CONTROL OBJECTIVES	AUDIT CONSIDERATIONS	Y	N	REMARK
To ensure that: a. Systems are developed according to Government Rules & Regulations. b. Government interest is taken care of in formulation of the contract. (* This contract should be referred to throughout the audit)	1.1 Information Strategic Plan exist. 1.2 Formation of ICT Steering Committee, ICT Technical Committee & Project Team. 1.3 Ensure that all Federal Circulars pertaining to the system development are complied with. 1.4 The deliverables at each phase are included in the contracts. 1.5 Transfer of Technology (TOT). Auditee's ICT personnel are able to maintain and measured the basic operation of the system. 1.6 Training. 1.7 Ownership. 1.8 Audit requirements: • Unlimited Access to the system • Audit trails • Embedded audit module • Security 1.9 Progress payment. 1.10Disaster Recovery Plan.			

B. INITIATION

CONTROL OBJECTIVES	AUDIT CONSIDERATIONS	Y	N	REMARK
To ensure that: 1. Systems developed are approved and implemented if they are justifiable for economic or other sound reasons.	2.1 Analysis of the project costs and benefits prepared to evaluate the economic feasibility of each alternative. • Costs & benefit analysis • Time & costs estimates • Impact study • Technological advance • User requirements • Risk for successful completion 2.2 The feasibility study reports are reviewed by ICT Steering Committee and that			

	decision has been made. 2.3 Resources required to support systems after being developed. 2.4 The project team should have the skill and time to accomplish all designated responsibility. 2.5 The existing system should be adequately reviewed: • Existing problem vs user needs • New system to be based on the review and the feasibility study			
C. SYSTEM ANALYSIS				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	**Y**	**N**	**REMARK**
Systems are developed according to approved plans and procedures.	3.1 Detailed statement of User Requirement Specification (URS): • Description of current problem • Narrative describing requirements of proposed system • System acceptance criteria • Involvement of all users • URS must be documented and approved by ICT Steering Committee 3.2 URS is translated into Functional Requirement Specification (FRS). 3.3 The URS are translated into logical and physical design/system. 3.4 The design are properly documented. 3.5 The conceptual system design should include the following: • Context Diagram • Entity Relationship Diagram • Data Flow Diagram • Processing times and general methods of operation • Interface manually and with			

	other systems • Responsibility for completeness and accuracy of data • User participation in design process 3.6 Physical design should include : • Physical flow • Hardware configuration • System flow • Files and data base specification • Computer programme specification • Input and report layout 3.7 To determine that the detail design includes all material items regarding the systems and the operations of the organisation: • File design should be consistent and all disk and tape files should be completely described and documented • Sufficient audit trails should exist and access controls should be well defined • Input formats & source documents are defined in detail • Validation provisions and operational controls on source documents and input (e.g. batching, balancing, edit checks) • Input, processing, output and operational controls should be adequate and properly documented • Outputs are defined in detail, should meet user needs (in terms of content usefulness) and also meets security provisions			

D. SYSTEM DEVELOPMENT				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	**Y**	**N**	**REMARK**
To ensure that design and development of the system reflect the user requirements.	4.1 Programming is completed according to the detailed design and has been adequately tested to conform with specifications. • Detailed systems and sub-systems specification should be developed for the systems. They should include: - an overall narrative description of the systems - the equipment configuration needed to process the systems - the systems software needed to support the systems - the interfaces with other systems - the security and privacy requirements of the systems - the operational controls over the systems - the design characteristics of the systems, including a system flowchart • Detailed programme specifications should be developed for all programmes of the systems. These specifications should include the following: - a general narrative description of the programme and its functions - the equipment required to operate the programme - the system software needed to support the programme - the storage requirements of the programme, including the amount of internal storage and the amount and type of offline storage the security and privacy requirements of the programme - the control over and within the programme lists of constants, codes and tables used - the operating procedures of the programme			

D. SYSTEM DEVELOPMENT				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	**Y**	**N**	**REMARK**
	- the input record formats and descriptions - a description of the programme's logic, including flowcharts and decision tables, supplemented by narrative explanations - the output record formats and description - the logical and physical characteristics of all data bases used by the programme, including file layout and data element definitions - source programme listing - object programme listing • Detailed specifications should be developed for databases used by the computer-based system. These specification should include the following: - the data base identification - the system using the data base - the labelling and tagging convention used when the data base is accessed - any special instruction for using it - the system software needed to support it - its logical characteristics - its physical characteristics			

D. SYSTEM DEVELOPMENT				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	**Y**	**N**	**REMARK**
	• Systems and programmes should be adequately tested by ICT personnel and should be acceptable to the users: - Detail development testing ▪ unit testing ▪ integration test ▪ system test - test data prepared to test the wide range of valid and invalid transactions. - test results to be reviewed and approved by users and ICT Technical Committee (results can be compared with planned or parallel system results) complete record of problems detected during testing - sufficient resources allocated to tests - formal systems acceptance procedures - sign off by users • System Documentation, such as users Manuals, Operational Manual are produced • Procurement of hardware and software according to specification • Training for various users delivered			

E. IMPLEMENTATION

CONTROL OBJECTIVES	AUDIT CONSIDERATIONS	Y	N	REMARK
To ensure that: 1. The management acceptance over the systems is secured. (Only tested and approved systems are accepted and established). 2. All programmes documentations, operation manuals and user manuals are complete and ready for use.	5.1 Detailed implementation plan is prepared to ensure adequate control is maintained during the conversion from the old systems to the new systems. • Detailed implementation plan to include phases such as, functional specifications, programming, testing parallel running, conversion, training and documentation, impact of hardware/software, site preparation and forms design • Formal procedures for approval and acceptance by all parties (management, ICT department, users) • Detailed conversion plan which cover systems testing, initial files creation, reconciliation, training of ICT and user personnel, time and manpower requirements, and instructions or user manuals • Adequate back-up is available to recreate files in the event there are problems encountered during conversion (unmatched totals, missing data, etc) • Pilot testing on the system prototype • Final acceptance test - stress test - volume test - security test • End user training are given			

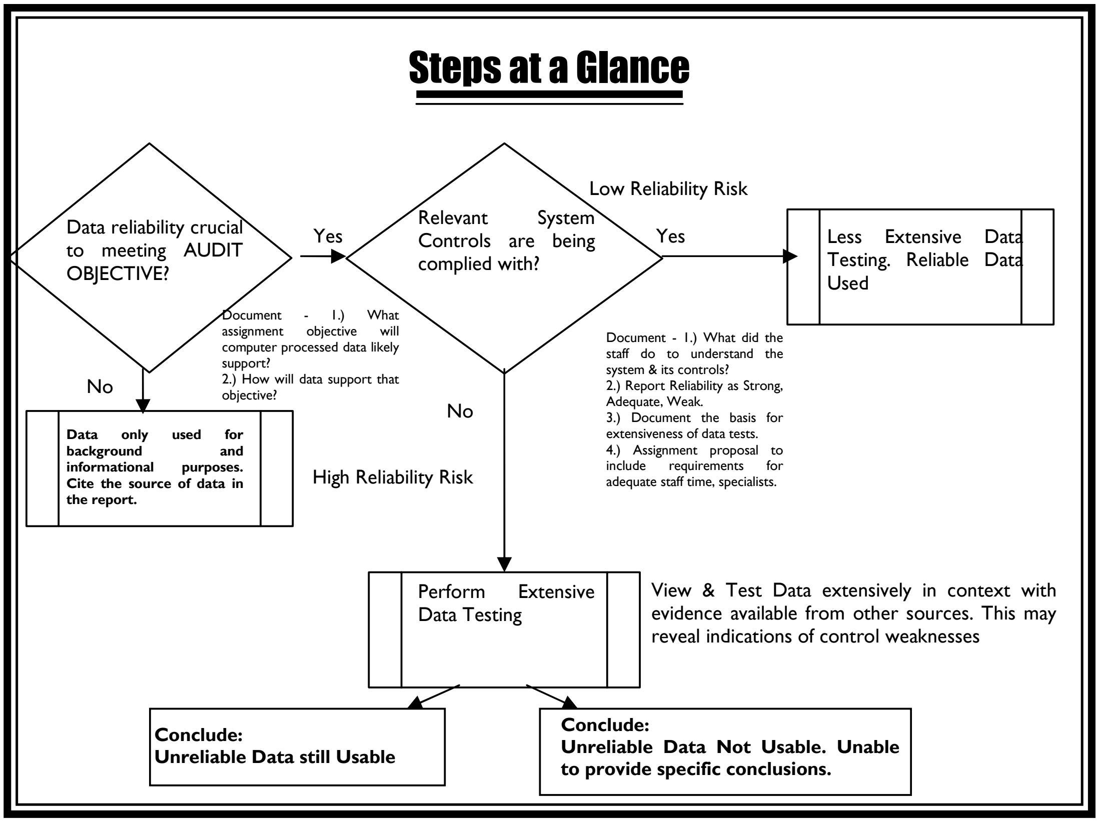
F. MAINTENANCE

CONTROL OBJECTIVES	AUDIT CONSIDERATIONS	Y	N	REMARK
To ensure that procedures are in place so that processing may be done smoothly and accurately. System modifications are appropriately	6.1 Cost of operation should be recorded, analyses and monitored. 6.2 Procedures to monitor and control system charges are established and record of the charges are properly kept.			

authorised.	6.3 Disaster recovery plan should be frequently reviewed and tested.			
G. POST IMPLEMENTATION REVIEW				
CONTROL OBJECTIVES	**AUDIT CONSIDERATIONS**	**Y**	**N**	**REMARK**
To ensure that systems meet user requirements and achieved their objectives.	7.1 The effectiveness of systems are regularly monitored and that system meets users requirement • Interviewing users • Reviewing output reports • Examination of computer usage reports • System response time • Examine error rates on edit and file maintenance report 7.2 Aspect of project management • Time over run • Cost over un • Performance standard met			

Appendix 4.1
[*Page 76*]

Understanding System Controls and Determining Data Testing Requirements



Steps at a Glance

Data reliability crucial to meeting AUDIT OBJECTIVE?

Yes

Relevant System Controls are being complied with?

Low Reliability Risk

Yes

Less Extensive Data Testing. Reliable Data Used

Document - 1.) What assignment objective will computer processed data likely support?
2.) How will data support that objective?

No

Data only used for background and informational purposes. Cite the source of data in the report.

No

High Reliability Risk

Document - 1.) What did the staff do to understand the system & its controls?
2.) Report Reliability as Strong, Adequate, Weak.
3.) Document the basis for extensiveness of data tests.
4.) Assignment proposal to include requirements for adequate staff time, specialists.

Perform Extensive Data Testing

View & Test Data extensively in context with evidence available from other sources. This may reveal indications of control weaknesses

Conclude:
Unreliable Data still Usable

Conclude:
Unreliable Data Not Usable. Unable to provide specific conclusions.

Glossary

Term	Definition
Application Controls	Refer to the transactions and data relating to each computer-based application system and are therefore specific to each such application. The objectives of application controls, which may be manual, or programmed, are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.
CAATs	Computer Assisted Audit Techniques. Any automated audit technique, such as generalised audit software, test data generators, computerised audit programs and specialised audit utilities.
CIS	Computerised Information System
Compliance Testing	Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period.
Depot	Downloading utility provided by Overland Data.
Fdump	Data display utility provided with Overland Data tape management.
General Controls	Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.
IAPS	International Auditing Practice Statements developed by IFAC. IAPSs are issued to provide practical assistance to auditors in implementing the ISAs or to promote good practice. These statements are not intended to have the authority of standards.
ICT	Information and Communications Technology. A generic term applied to the technology required for information processing. In particular the use of electronic computers to convert, store, process, transmit, and retrieve information.
IFAC	International Federation of Accountants.

Term	Definition
IIA	Institute of Internal Auditors.
ISACA	Information Systems Audit and Control Association. The global professional organisation for Information System auditors.
ISAs	International Standards on Auditing (ISAs) developed by IFAC. National standards on auditing published in many countries differ in form and content. IFAC takes cognisance of such documents and differences, and, in the light of such knowledge, issues ISAs, which are intended for international acceptance. ISAs are to be applied in the audit of financial statements. ISAs are also to be applied, adapted as necessary, to the audit of other information and to related services.
ISO17799	An international standard that defines information confidentiality, integrity and availability controls.
Risk	The possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems.
SDLC	System Development Lifecycle. An approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review.
Tapeutl	scanning/downloading utility provided by Flagstaff Engineering
Tarsus	Downloading and extraction utility by Memory Technology.
Vulnerabilities	Weaknesses in systems that can be exploited in ways that violate security policy.