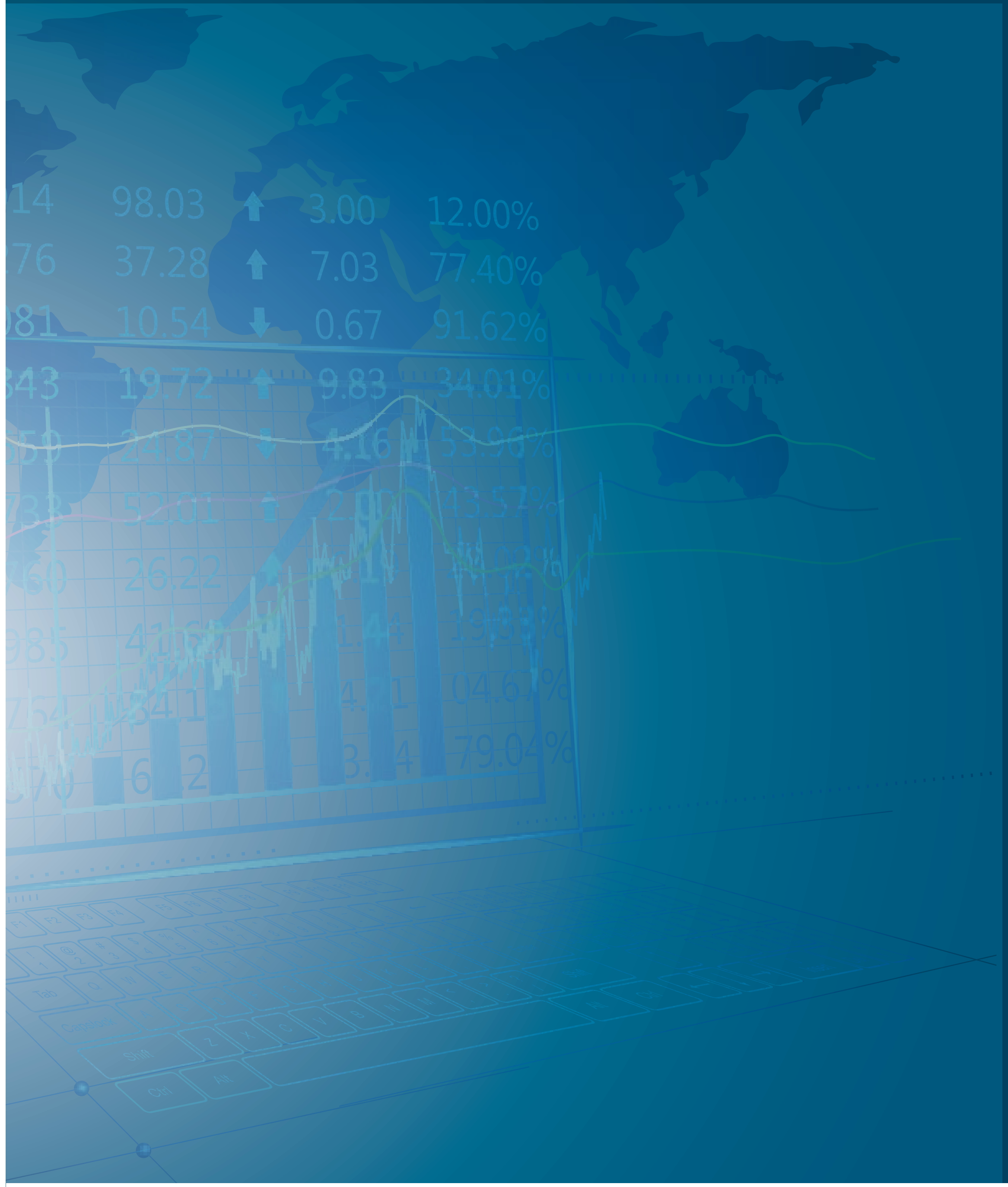


SPEMP

Strengthening Public Expenditure Management Program

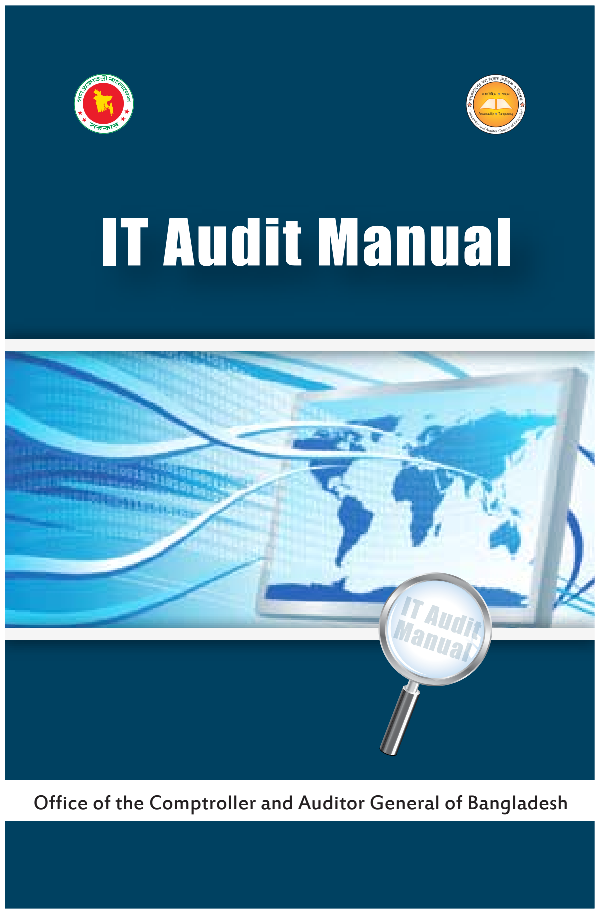
MAKING PUBLIC MONEY COUNT

SPEMP-B : Strengthening the Office of the Comptroller and Auditor General
Address : Audit Complex (11th Floor), Segunbagicha, Dhaka-1000
Phone : +88 02 8391274-77, PABX : +88 02 8391277
Fax : +88 02 8391276

IT Audit Manual

IT Audit Manual

Office of the Comptroller and Auditor General of Bangladesh



IT Audit Manual

Office of the Comptroller and Auditor General of Bangladesh

FOREWORD

Introduction of IT Audit in the Supreme Audit Institution (SAI) of Bangladesh has been a long felt need. To meet that need, this manual has been developed to guide the audit teams in conducting quality audits. The manual intends to make some contribution towards modernisation of auditing practices and improving the quality of audit by introducing IT audit.

As the first step towards building the IT capacity of OCAG, an IT Strategic Plan was developed. This manual has been prepared in line with the IT Strategic Plan. Top priority was therefore given to IT auditing, specially in view of the stated government policy of achieving the goal of 'Digital Bangladesh'.

This Manual, I hope, will be instrumental to the auditors in understanding and carrying out IT Audit. The manual, being a guide to IT audit, will enhance capability and skill level of the auditing staff to carry out effective IT audit.

The manual should be read along with the Government Auditing Standards, the Audit Code and other Audit Manuals issued by the Office of the Comptroller and Auditor General of Bangladesh as well as International Standards on Supreme Audit Institutions (ISSAIs). All procedures and techniques set out in these documents, as far as they relate to IT audit, should be followed with due care.

I am confident that the manual will be a valuable addition to the knowledge and experience for the officials of the department in conducting IT audit. In the field of Information Technology, the changes are rapid and as such the manual will be updated from time to time to accommodate organisational and legislative reforms as well as emerging trends of audit tecniques and methodologies. Any suggestion for improvement of this manual will graciously be accepted.

I am particularly thankful to the DFID funded Financial Management Reforms Programme (FMRP) Project for the initial works in preparing this manual. I am also appreciative of the Canadian International Development Agency (CIDA) funded SCOPE (Strengthening Comptrollership and Oversight of Public Expenditure) Project for developing necessary IT infrastructure and capacity building for IT audits.

My special thanks go to SPEMP-B Project for their utmost sincerity and cooperation in revising , updating and finally printing the **"IT Audit Manual"**. We hope that this IT Audit Manual will be useful in making quality IT Audits.

Dhaka
Nov 23, 2015

Masud Ahmed
Comptroller and Auditor General of
Bangladesh

Contents

Introduction

1. The Comptroller and Auditor General (C&AG) is appointed by the President and is the Head of the Supreme Audit Institution (SAI) of Bangladesh. The authority of the C&AG to carry out all types of audit is derived from Article 128 of the Constitution of the People's Republic of Bangladesh and the Comptroller and Auditor General (Additional Functions) Act, 1974. This legislation empowers the C&AG to audit the public accounts of the Republic and, for that purpose, to have unrestricted access to all records, books, vouchers, documents or other items required for the audit.

2. IT auditing can make a significant contribution to the ability of the Office of the C&AG to fulfil this mandate. This audit manual contains the policies and procedures necessary for the promotion, development and conduct of IT auditing throughout the Audit Department.

Purpose of the IT audit manual

3. The objectives of this audit manual are:

- To provide advice to general and specialist auditors on the principles and techniques to apply when planning, managing and performing IT audit work.
- To ensure that IT audit work is carried out consistently and efficiently and in accordance with International Organisation of Supreme Audit Institutions (INTOSAI), Asian Organisation of Supreme Audit Institutions (ASOSAI) and other recognised international standards and guidelines.
- To promote the integration of IT auditing within the other activities of the Office of the C&AG.
- To provide sample documentation for use during IT audit work.
- To provide the basis for future IT auditing training.

Scope of the manual

4. Some issues common to all audit services are included in separate audit manuals. Where this is the case only special considerations relating to IT auditing are included in this manual.

General approach in compiling the manual

5. The overall approach to the establishment, promotion and development of IT auditing needs to be practical if it is to integrate fully with other audit services. This document is aimed primarily at providing audit staff with the basic theory necessary to achieve a major increase in audit coverage and effectiveness through the implementation of IT auditing. The contents of this manual will be supported by further, more practical, training at the inception of IT audit work.

Structure of the manual

6. The manual comprises the following sections:
   - Role and framework;
   - Planning of IT audit work;
   - Conduct of IT audit control reviews;
   - Information Systems Development;
   - The use of computer assisted audit techniques.

Sources

7. This manual draws upon material originally published by various organisations including the INTOSAI, ASOSAI, the Information Systems Audit and Control Association (ISACA), the UK Chartered Institute of Public Finance and Accountancy (CIPFA), and the Supreme Audit Institutions of the United Kingdom, Canada and New Zealand.

Revisions to the manual

8. This manual should be reviewed regularly and amended to reflect changes in business needs, and technology as well as audit techniques and staff skills. All relevant staff should be provided with details of revisions to the manual.

PART A

The IT Audit Framework

This section deals with the following:

- Definition of IT auditing
- The impact of computers on control and audit
- The need for IT auditing
- The development of IT auditing within the Office of the C&AG
- IT auditing standards
- Overall objectives for IT auditing
- Responsibility for IT audit work
- Training for IT auditing
- The application of IT auditing within the Office of the C&AG

Appendix A.1:The impact of computers on control and audit

Definition of IT auditing

1. IT auditing has been defined as "the process of collecting and evaluating evidence to determine whether an information system has been designed to maintain data integrity, safeguard assets, allow organisational goals to be achieved effectively and use resources efficiently" (ASOSAI IT Audit Guidelines).

2. IT auditing embraces the independent reviewing and testing of the organisation's practices and procedures relating to:

    - The processes for developing and acquiring new IT systems and facilities;
    - Internal controls within the IT environment to assure validity, reliability and security of information;
    - The economy, efficiency and effectiveness of the use and exploitation of IT facilities.

The impact of computers on control and audit

3. Computer technology has significantly impacted the control and audit process. Although control and audit objectives generally remain constant, technology has altered the way in which systems should be controlled. Technology has impacted the audit profession in terms of how audits are performed. Auditors now need specialised technology and knowledge to perform their duties efficiently and effectively. Computers introduce:

    - New risks;
    - New causes of error;
    - Missing audit trail or evidence;
    - Changed internal control;
    - The need for modified audit procedures.

4. The attached Appendix A.1 considers these issues in more detail.

The need for IT auditing

5. IT auditing capacity and capability is needed within the Office of the C&AG for the reasons set out in the following paragraphs.

6. Firstly, information technology is growing in importance to the Government. The Government of Bangladesh targets effective use of information and communication technology through formulating a 'Digital Bangladesh' vision in establishing an efficient, transparent and accountable government. A number of major systems are already computerised and the pace of IT development is likely to accelerate. IT auditing techniques are needed to assess the resulting changes in the location and nature of internal controls and to ensure that the government meets its organisational and IT objectives including the need for the confidentiality, integrity and availability of information and compliance with legal and statutory requirements. IT auditing is essential to provide assurance that system of internal control for information technology are likely to result in the production of accurate financial information and statements.

7. IT auditing also provides the C&AG and his staff with opportunities to improve the efficiency and quality of its audit services by:

   - Improving the overall control structure and enabling better targeting of audit resources;
   - Introducing computer assisted audit techniques and tools (CAATs) designed to automate the process of identifying potential weaknesses, save general auditor's time and improve the quality of individual audits;
   - Providing support for the introduction of other audit methods and techniques such as systems based auditing.

IT auditing standards

8. All staff engaged in IT auditing work must comply with Government Auditing Standards. In addition, IT auditors should have regard to INTOSAI Auditing Standards, International Federation of Accountants (IFAC) Auditing Standards and those of professional IT audit bodies such as the Information Systems Audit and Control Association (ISACA), and The Chartered Institute of Public Finance and Accountancy (CIPFA) Computer Audit Guidelines.

9. IT auditors must maintain their independence. The audit report and opinion must be free from any bias or influence. IT auditors must at all times maintain control over the direction and content of IT audit work undertaken, collect evidence independently wherever possible (e.g. using audit software or by via third parties) and form their own conclusions and recommendations about the adequacy of controls based upon an impartial evaluation of the audit evidence.

Overall objectives for IT auditing

10. The OCAG Information Technology Strategic Plan (2010-2014), and the Information Technology Policies issued by the C&AG sets out the overall IT objectives for the OCAG.

These are included in the following statement of the objectives of IT auditing:

- Develop in-house capacity in auditing in information technology environment to increase OCAG's effectiveness as a Supreme Audit Intitution;
- Carry out effective evaluations of the internal controls built into existing information systems;
- Provide advice concerning the audit aspects of information systems being developed with a view to ensuring that valuable development resources are not wasted and that the internal controls implemented result in accurate financial statements;
- Promote the more effective use of CAATs and other IT based audit tools within the Audit Department;
- Support the implementation of other changes in audit methods and techniques (e.g. Risk and Systems Based Auditing).

Responsibility for IT audit work

11. The IT Steering Committee chaired by the C&AG and including other senior audit managers is responsible for supervising, monitoring and directing the IT related activities of the Audit Department. Senior audit managers within each audit Directorate are responsible for the promotion and development of IT auditing within their areas of control.

12. Two categories of staff will review IT controls:

- A small, central team will review IT infrastructure and application controls with a view to improving internal controls and identify the degree to which other auditors can rely upon their work.
- Auditors situated in each audit directorate will assess and test the operation of manual controls associated with IT systems as well as provide support to the central team.

13. IT auditors, particularly those in the central team, should co-ordinate their work with the staff maintaining the C&AG's management information systems with a view to promoting, implementing and operating CAATs.

Training for IT auditing

14. Selected auditors within each audit directorate will be provided general appreciation of IT controls and be trained in the use of IT control checklists. The smaller number of specialist IT auditors will require more advanced IT audit training.

The application of IT auditing within the Office of the C&AG

15. IT auditing techniques can be applied in the implementation of financial, performance and information systems development audits. The audit objectives for an individual IT audit will vary according to the nature and category of the audit.

16. The purpose of a financial audit is to express an opinion on the financial statements and accountability of audit entities. Where IT auditing is carried out to support financial auditing the primary objective will be to provide assurance that financial statements produced from an information system reflect a true and fair view of the entity's financial position. The objectives of carrying out IT audit work as a component of a financial statement audit includes expressing opinions on:

    - How well management uses ICT to improve its business processes;
    - The way in which information technology is used for the storage and processing of financial information and the impact upon internal controls;
    - The controls that management uses to measure, manage and control information technology;
    - The effectiveness of information technology controls that impact on the processing of financial information.

17. The purpose of a performance audit is to evaluate the efficiency, economy and effectiveness of audited entities. For performance audits, IT audit objectives will depend upon the role of IT within the audit:

    - If the performance audit is of the use of information technology itself the audit objectives will include examining the organisation's IT systems and how they are performing against benchmarks.

    - Where an IT audit is a component of a wider performance audit, the IT auditor will typically be required to evaluate the impact of IT upon the processes of the service being reviewed, provide assurance that the IT systems can be relied upon to play their part in delivering the service efficiently and effectively, and extract appropriate data held in IT systems.

18. Information systems development audits ensure that there are sufficient and appropriate controls over the entire IT development life cycle from system initiation to live operation. IT audit objectives include:

- Projects are subject to a full business justification;
- Development objectives are clear and achievable;
- The project is well managed and controlled;
- Pre-specified development standards are applied;
- Future technology improvements are considered;
- The new system includes sufficient and appropriate controls;
- New systems are subject to post-implementation review.

19. Ultimately, the expectation is that the Office of the C&AG will be able to deliver a full range of IT control reviews and use all appropriate CAATs. Initially, the focus will be upon:

- Undertaking reviews of basic IT controls as part of financial statement and performance reviews;
- Building up expertise in the use of Computer Assisted Audit Techniques (CAATs) and Tools .

Appendix A.1

The impact of computers on control and audit

General

1. A manual system is based on hand written books of account, manual procedures.

2. Computers do not alter the objectives of audit. However, they result in the need for:

    - Audit trail changes
    - Changes in internal control
    - New causes of error
    - New audit procedures.

Changes in audit trail

3. Where information systems are introduced the audit trail and audit evidence traditionally associated with manual systems is often missing. Computers typically impact upon audit trail and audit evidence in the following ways:

Audit trail/evidence	Impact upon audit	Example
Transaction audit trail	May be disguised in machine readable form.	Transactions held in a computer file
	The link between input and output may be harder to follow	Where an output value is calculated by a computer programme from two inputs
	May not be retained	Computer file contents may be temporary
	Retention period may be inadequate	Computer file archiving duration may not reflect legal retention requirements
Audit evidence	New transaction types	Computer transaction control records may provide valuable audit evidence
	May originate in the computer	Where a computer creates and maintains audit trail records
	No formal authorisation	Where calculation is automatic

Changes in internal control

4. Computers impact on the seven main categories of internal control in the following ways: -

Categories of Internal control	Impact upon audit
Competent and trustworthy personnel with clear job descriptions	· No special considerations
Adequate segregation of duties	· Concentration of functions · Concentration of knowledge
Proper authorisation procedures	· Transactions originate inside the computer · Computer programmes control transactions
Adequate documents and records	· Lack of visible transaction trail
Proper record keeping procedures	· Centralisation of programmes and data · Consistency of performance

Physical control over assets and records	· Portability of hardware · Machine readable nature of backup copies · Special requirements for data and programme storage
Independent performance checks	· No special considerations.

New causes of error

5. Computers also introduce a number of new causes of error not met in traditional manual systems . These include:

New causes of error	Example
Computer-generated transactions	A total cost calculated automatically and based upon a quantity and a unit price.
Systematic error	An incorrect accounting code in a table will result in an error for all transactions using that code.
Larger impact of small errors.	A minor typing error in a table of unit prices will result in a larger error when multiplied by quantities to calculate total costs.

New audit procedures

6. Finally, computers introduce the need and opportunity to adopt revised audit procedures for a variety of reasons including:

New audit procedures	Example
Changes in audit trail	Computer records can provide details of user names authorising transactions.
Changes in internal controls	Preventative controls can be built into computer systems e.g. the requirement that amounts input must be within a pre-defined range.
Opportunity to apply better testing.	Computer Assisted Audit Techniques (CAATs) and tools can analyse 100% of transactions in a computer system in less time than a small manual sample can be tested.

PART B

Planning IT Audit Work

This section deals with the following:

- Introduction to IT audit planning
- IT audit planning objectives
- Business risks in a computerised environment
- The Medium Term Strategic IT audit plan
- Annual IT audit plan

Appendix B.1: Risk Analysis, Audit Needs Assessment & IT Audit Planning

Introduction to IT audit planning

1. If coverage is to be adequate and IT audit resources are to be used efficiently and effectively then it is essential to plan all IT audit work to be carried out. This section therefore deals only with those aspects of the IT audit planning process that are different to those for other audit services or that need special emphasis.

2. The IT audit planning should be part of medium term strategic IT audit plan (3 to 5 years) which is also a part of OCAG's overall medium term strategic audit plan on which annual audit plans should be based.

IT audit planning objectives

3. For IT audit these differences include:

- To ensure that IT audit work reflects business risks and the priorities of the Office of the C&AG and its clients;
- To identify resource and training mismatches and their resolution;
- To integrate IT and other audit work so as to provide the maximum audit coverage and efficiency.

Business risks in a computerised environment

4. No audit team has enough resources to achieve 100% review of all areas. Therefore priorities should be given according to their relative risk. Business risks within a computerised environment include:

- Computer applications that do not meet the needs of the organisation;
- Unauthorised modification;
- Loss of data accuracy;
- Unauthorised access to and/or disclosure of data;
- Lack of continuity of service;
- Waste of development resources.

The Medium Term Strategic IT Audit Plan

5. A medium term strategic IT audit plan should be prepared by the central IT audit team based upon a formal audit risk analysis and needs assessment and information provided

by each Director General. On completion the plan should show the frequency with which each audit is to be carried out and the time required to complete each audit as well as the total time required to complete each year of the plan. It should be updated annually and form the basis of annual operational audit plans.

6. When compiling and updating the medium term IT audit plan it is particularly important to involve auditees fully. It is also important to involve other audit staff if there is to be greater harmonisation between the work of specialist and other auditors.

7. A practical approach to the preparation of a medium term IT audit plan is described in detail in the attached Appendix B.l. Many of the steps can be analysed using the formulae of a spreadsheet that helping to automate this activity and save time.

8. As part of the process of preparing a medium term IT audit plan an audit risk analysis and needs assessment will need to be carried out. The objectives of the audit risk analysis and needs assessment are to:

- Identify all the areas to be audited
- Assess their relative risks
- Determine the period over which systems will be audited
- Allocate frequencies to audits
- Estimate the resources required to meet audit needs.

9. The allocation of projects over the five years of the strategic plan should be such as to provide a balance between:

- Generic reviews
- Data centre/general controls reviews
- Existing computer applications
    - core financial systems
    - system support to core financial systems
    - major departmental systems
    - minor departmental systems
- Enhancements to/new applications
- Advisory/consultancy services
- Indirect time

10. Once the draft medium term IT audit plan has been prepared it should be integrated with

other non-IT audit services to identify whether IT audit will be executed on a stand-alone basis or part of general audit. The availability and capability of resources, geographical location and OCAG's approach will determine the stand-alone or integration decision.

11. Appropriate performance measures should be produced regularly (e.g. monthly) to monitor and minimise unplanned work to which computer audit is susceptible (performence measures should be exemplified).

12. The medium term IT audit plan should be updated regularly. Information technology and its use changes rapidly. Although this does not diminish the need for a medium term planning process it does mean that the resultant plan may be more subject to change than that for other audit services. Because of this it is important that there are formal arrangements, perhaps in the form of periodic (say quarterly) meetings, with the clients who are the main IT users to ensure that audit is notified regularly of any changes likely to affect the medium term IT audit plan.

Annual IT audit plan

13. The medium term strategy should be revised each year to take account of changes in the audit inventory, relative risks and audit policies. Each year the first year of the medium term strategy should be adopted as the next annual audit plan.

14. The annual IT audit plan therefore contains the audits to be carried out in the current audit year to fulfil the medium term strategic IT audit plan. The annual plan should contain each audit to be carried out, details of the relevant risk factors and the time allocated to each audit and details of the staff allocated to the individual audits.

Appendix B.1

Risk Analysis, Audit Needs Assessment & IT Audit Planning

Summary

1. The following steps will need to be followed in carrying out the audit risk analysis and needs assessment:

- Identify all the potential areas to be audited for each client
- Identify the risk associated with each area (see Section 6 below)

2. Decide on the audits for the next 3 years

- Estimate the time required achieving each audit
- Allocate the audits over the strategic plan period
- Summarise the audit needs by service and audit type
- Estimate the level and type of resources required to achieve the 3 year medium-term strategic audit plan.

Compiling the preliminary computer audit inventory

3. The first step is to:

- Compile a preliminary list of all audit areas that need to be covered. In this context an audit area is an individual client for whose accounts the C&AG is required to provide assurance. In the case of the government each system operating in the ministries/departments should be considered a separate audit area.

4. The next step is to compile a list of audits to be carried out for each audit client. The inventory of potential IT audit work should cover all IT facilities within the organisation. In order to achieve this potential audits should cover:
   - Generic (specific) reviews covering areas of potential benefit to all Divisions (e.g. IT acquisition procedures, Life Cycle Development (including change control), Network Security, etc.
   - Control reviews of the data centre(s) processing the core, corporate computer applications
   - Divisional computer control 'health checks'
   - Control reviews of existing corporate and divisional computer applications
   - Control reviews of computerised financial systems under development
   - Measures to increase audit automation and improve audit productivity.

5. The list of potential audits should be sent to the Directors General (DGs) requesting that they amend the list by adding any new or other areas that have been omitted and excluding any area that no longer exists.

6. Regular and formal means of communication should be established to ensure that the audit inventory is updated periodically to reflect new processing arrangements, the withdrawal or enhancement of existing applications and the development implementation of new applications.

Risk analysis

7. Ultimately, resources should be allocated according to risk and this requires that a formal risk analysis be carried out for each area covered by the audit inventory. The steps in compiling a risk analysis are:
   - Obtain an understanding of the area so that its associated audit risk can be identified;
   - Establish the risk factors to be used;
   - Devise scoring methods to be used for each factor;
   - Devise a weighting factor for each risk factor;
   - For each audit area ascertain the scores for the risk factors;

- Automate the calculation of weighted total risk scores and the ranking of audit areas as high, medium or low risk according to predetermined scoring ranges;
- Determine the frequency of audits (i.e. every one year, two years, three years, etc.) according to the level of risk associated with each area included in the IT audit inventory.

8. There is no 'perfect' set of risk factors for use as part of a risk analysis but the following should be considered for inclusion:

(a) Materiality

This refers to the overall value of the information assets concerned.

(b) Last audit examination

This refers to the time elapsed since the audit area was last reviewed. This also includes prior audit findings.

(c) Value

This refers to the annual value of the transactions of the service. The estimated expenditure should be added to the estimated income to arrive at a total.

(d) Transaction volume

This refers to the number of financial transactions carried out by the service in a year.

(e) Complexity of the processing environment

This refers to the inherent risks in the processing environment.

- How many processors are involved? Number of platforms
- Is processing centralised/devolved or decentralised? Batch or real time processing
- Number of users, size of the system
- Number of system's modules and interfaces.

(f) Vulnerability

This is a judgment as to whether the features of the service make it vulnerable to loss, corruption, fraud or error.
In making an assessment the auditor must make a judgement as to whether the service has high, medium or low vulnerability taking into account the following examples:

- Is the system stable?
- Is there a history of poor control?
- Are there known system weaknesses?
- Does it require a high level of internal control?
- Does it allow ease of access to cash?
- Is the information of value?
- Is there an opportunity to convert the information into cash?
- How complex is the system in terms of the skills required to maintain it?

(g) Sensitivity/criticality

This is an assessment of the damage or embarrassment that may be caused if there were to be unauthorised loss of processing continuity or, alternatively, loss, modification or disclosure of data. It can be measured from no impact to high impact.

(h) System management and governance

This includes in-house development or outsourcing develpment, governance and management structure, numbers and skills of human resources, changes of human resources (low to high turnover), written policies and procedures.

9. Each risk factor should be given a weighting according to its relative importance. The weight factor (between 1 and 10) for each risk factor will be subjective to some extent and will represent the knowledge and expertise of senior audit staff.

10. Based on the risk factor scores and weight factors, the formula to arrive at the weighted total score for each audit area is as follows where the alpha characters represent the scores allocated for the various risk factors and the numbers represent indicative, respective weightings:

$$a8.75+b6.5+c9.0+d4.75+e5.5+f7.5+g8.5+h5.5/560*100$$

Alternative method

Each area in the IT audit inventory can be rated on the above risk factors using a numeric risk value ranking of 1 (low) to 5 (high). These ranking results are multiplied by a weight factor ranging from 1 (low) to 10 (high) to find an extended value for each risk factor. These extended values are added together to find a total risk score for each area. Thus the simple formulae will be arrived as follows:

Total score = 9a+7b+9c+5d+6e+8f+9g+5h

In addition to above methodologies, the analysis team can use any other recognised methodology for this purpose. Whatever methodology is chosen it should be used consistently throughout the analysis process.

11. This produces a risk 'score' for each audit. Ranges of raw scores should then be classified as high, medium or low risk according to scoring range. Each audit should be allocated to one of these categories depending upon its risk score.

Audit needs assessment

12. All risk analysis data collected will be input to a spreadsheet to calculate the total weighted score for each audit area.

13. Audit areas will be ranked according to high, medium and low risk areas in order to determine the required frequency of audits based on the following weighted total scores:

High risk area	-	Every 1 to 2 years
Medium risk area	-	Every 2 to 3 years
Low risk area	-	Every 3 to 5 years

14. When deciding which audits should be carried out in each of the next 5 years, the date of the last audit and any specific management concerns of clients should be taken into account. The allocation of the days allowed for each audit to the appropriate year results in a 5 Year Strategic Audit Plan.

15. The risk analysis and audit needs assessment should be updated at least annually in order to include or exclude new areas or systems or to accommodate changes in risk levels and/or increase in audit productivity.

PART C

IT Control Auditing

This part deals with the following:

- C1: The overall approach to IT control auditing
- C2: Reviewing the general controls at computer installations
- C3: Procurement of IT facilities
- C4: Reviewing existing computer applications
- C5: Major enhancements and new application under development
- C6: Data conversion reviews

PART C1

The overall approach to IT control auditing

This section deals with the following:

- Introduction
- IT controls
- Consequences of lT control failure
- Conducting IT control audits
- The preliminary survey
- Assessing risk in a computerised environment
- Planning individual IT control audit
- Information systems control objectives
- Recording the system
- Evaluating the system design
- Compliance tests
- Substantive tests
- Reporting
- Review and quality control

Appendix C1.1: The steps in system based auditing

Introduction

1. A number of major government agencies have implemented IT based information systems including the Controller General of Accounts (CGA), the National Board of Revenue (NBR), nationalised commercial and specialised banks, Bangladesh Railway and other service sectors. The increased uses of information systems in the government agencies require that these systems are adequately controlled and secured, records are accurately maintained and risks are acceptably reduced.

IT controls

2. The controls within an information system comprise all of the manual and programmed methods, policies and procedures that ensure the protection of the entities assets, the accuracy and reliability of its records and the operational adherence to management standards. IT controls form part of the overall internal control structure of an entity and are classified in the following three categories:

Control classification	**Control description**
General	These controls create the environment for the operation of the IT infrastructure and are not specific to particular applications. Control categories include IT policies, procedures and standards, operational controls, physical, programmed (logical) access, acquisition and business continuity and disaster recovery controls.
Application	Application controls refer to specific computer applications. This includes controls over the input of transactions, processing, output, and standing data.
Specific	These controls include Network and Internet, End user computing and IT Security.

3. Within this framework individual computer controls may be categorised as either:

- Programmed i.e. built into information systems themselves; or,
- Manual i.e. procedures operated to compensate for a lack of built in controls.

4. The stronger programmed controls, the less compensatory manual controls are required.The balance between programmed and manual controls should be such that the desired control level is achieved in the most effective and economic way.

5. Controls may be further categorised as preventative, detective or corrective. Preventative (often programmed) controls are to be preferred subject to being economically justified.

6. Wherever it is economic to do so, IT auditing should promote the implementation of programmed and preventative controls. These are best built into information systems at the development stage. This is less expensive than seeking to change, for example, a computer application after it has been implemented or to operate a compensatory manual control.

Consequences of IT control failure

7. These are significant and include:

- Computer applications inappropriate to business objectives
- Unauthorised modification of data
- Loss of data integrity
- Unauthorised access to and/or disclosure of data
- Lack of continuity of service
- Wasted development resources.

Conducting IT control audits

8. IT control audits should be primarily risk and system based. The main steps are repeated for convenience in the attached Appendix 1 to Part C 1. Within an IT auditing context the main steps are summarised below:

- Conduct a preliminary survey to obtain:
    - a broad understanding of the system and its boundaries
    - an indication of the main risk areas
- Assess the relevant risks
- Plan further IT audit work based upon the results of the risk analysis
- Identify control objectives and expected controls

- Document actual controls against expected controls
- Conduct a preliminary evaluation
- Devise and conduct audit tests
- Agree recommendations with the client
- Report as appropriate.

The preliminary survey

9. For each entity (e.g. a Ministry or Statutory body) the planning phase should include a preliminary evaluation of IT systems including:
   - Organisation of the computer function;
   - Use of computer hardware and software;
   - Applications processed and their relative significance;
   - Methods and procedures for making changes to existing, and for developing new, applications.

10. The preliminary survey will provide the basis for assessing:

    - The risks associated with the IT facilities of the relevant audit entity;
    - The potential for the use of CAATs both to test internal controls and to improve the quality of testing carried out by financial auditors.
    - The implications for other non-IT audit work (e.g. poor controls suggest the need for more substantive work by financial auditors to test account balances).

Assessing risk in a computerised environment

11. IT audit resources need to be directed to the areas of greatest risk in supporting the issue of an audit opinion on the entity.

12. There is no 'perfect' set of risk factors for use as part of a risk analysis in a computerised environment but the following risk factors need to be considered for inclusion:

    - The value of the transactions processed by the system;
    - The extent to which the organisation depends upon the correct running of the system. Note that a non-financial system may score more heavily than a financial system. For systems under development the score should reflect corporate priorities;

- The vulnerability of the system in terms of its stability, any history of poor control, known system weaknesses, required level of internal control, complexity, etc;
- Management's own assessment of the risks to the organisation if confidential information was disclosed or substantial losses occurred or there was a failure in the system.

Planning individual IT control audits

13. Depending upon the findings of the preliminary survey, the IT auditor will need to exercise their audit judgment to decide whether it is necessary to carry out further IT audit work to provide the necessary assurance.

14. Each IT control audit must be carefully planned. In particular:

- Audit scopes should not be so wide and unrealistic as to invite failure, loss of credibility and demoralisation;
- Unplanned work should not be allowed to undermine planned work (this does not preclude a revision of priorities);
- When planning IT audit work full recognition should be given to the fact that much IT-related audit work can be carried out by general auditors with a basic appreciation of IT controls and auditing (assessing the manual controls around a computer system);
- Wherever possible joint computer and financial audit input should be encouraged to promote the integration of audit services.

15. Parts C2 to C6 below include further details relevant to various types of control review and provide the basis for the development of individual audit programmes:

Type of IT Control Audit	Part
Reviewing the general controls at computer installations	C2
Procurement of IT facilities	C3
Reviewing existing computer applications	C4
Major enhancements and new applications under development	C5
Data conversion reviews	C6

16. Most computer control review work will be carried out using the systems-based audit (SBA) approach. The attached Appendix to Part C.l summarises the SBA approach. The remainder of this section considers particular issues that are likely to arise when applying SBA techniques to IT audit control reviews.

Information Systems Control Objectives

17. In order to facilitate the identification of controls the auditor should determine what the objectives of a sound control environment ought to be in relation to the system under examination. In doing so the IT auditor should take general control objectives and translate them into specific Information Systems Audit procedures.

18. Examples are:

- Information secured
- Transactions authorised and entered once
- Completeness of input in proper period
- Duplicates reported
- Rejections reported
- Adequate back-up
- Software change control.

Recording the system

19. The auditor must record the system before evaluation can take place. There is a variety of recording methods available including:

- Narrative
- Outline Flow Charts
- Detailed Flow Charts
- Questionnaires

20. Each method has its advantages and disadvantages and they are usually used together. For example, a system could be flowcharted in summary, selected processes described in more detail and in narrative, and questionnaires used to ascertain and provide information to evaluate internal controls.

21. It is important that the auditor should record the controls as well as the processes. Not all processes found in a system are necessarily relevant to the purposes of the audit examination; some may duplicate controls.

22. One approach, aimed at saving valuable audit time, is to concentrate on 'key' controls. Under this approach the lists of control objectives are sometimes referred to as 'key control questions' (KCQs). The concept of what is a key control in any given circumstance will be a matter of audit judgement. Usually, a key control is one that is essential for the achievement of the control objective and that is always present, for which evidence of its operation can be obtained and on which the auditor intends to rely.

Evaluating the System Design

23. The auditor must consider whether the control objectives will be achieved by the identified controls. It is necessary to establish whether the controls will, under reasonable circumstances, prevent and/or detect errors. If so then the auditor will proceed to conduct compliance or substantive tests.

Compliance tests

24. These are audit tests designed to confirm that controls have been operated as intended. Usually the auditor will only test key controls i.e. those which are relied on to meet control objectives.

Substantive Tests

25. All audits will require some substantive tests. These are carried out on individual transactions and seek to establish their correctness. Where auditors have identified a strong system which is operating correctly they will carry out substantive tests on a smaller number of transactions as they may draw some of the evidence needed to support the audit opinion from the system evaluation and compliance test results.

Reporting

26. The usual audit reporting processes should apply for all IT audit work. An IT auditor will report on the following matters:

   - Whether the system is capable of meeting the control objectives and, if not, in what respect;

- Whether any identified weaknesses have given rise to errors;
- Whether controls are being operated as intended;
- Whether any specific errors have been discovered and the likelihood of further undiscovered errors being present.

27. Reports will usually include constructive and practical proposals for dealing with any weaknesses discovered and avoiding errors in future.

Review and quality control

28. IT audit work needs to be subject to the same degree of quality control as other audit work.

Appendix C1.1

The steps in Systems Based Auditing

Step 1 Confirmation of the scope of the audit.
Step 2 Familiarisation with the entity to be audited.
Step 3 Review of previous audit papers.
Step 4 Preliminary planning:

- audit approach;
- staff allocations;
- timing;
- appointment with responsible officer.

Step 5 Pre-audit work:

- analytical review;
- assemble records held centrally needing to be tested on site;
- CAAT samples, where appropriate.

Step 6 Ascertain and record the system:

- prepare or update systems documentation;
- perform walk-through tests.

Step 7 Identify controls and perform the preliminary assessment (Evaluation of system design and preliminary risk assessment).
Step 8 Plan and perform tests of control.
Step 9 Evaluate test results (Evaluation of system operation) and design weakness test procedures if necessary.
Step 10 Evaluate weakness test results (Evaluation of results of system weakness).
Step 11 Summarise findings in the audit job report and prepare a draft for discussion.
Step 12 Discuss findings and recommendations with the responsible manager and agree action.
Step 13 Finalise audit report or management letter.
Step 14 Review and assessment of audit file:

- quality control review;
- amendment of audit programmes;
- follow-up items.

PART C2

Reviewing the general controls at computer installations

This section deals with the following:

- Introduction
- Risk
- Overall Audit Objectives
- Areas of Audit Interest
- Typical control Issues
- Organisational controls & Personnel issues
- Segregation of duties
- Operational controls
- File & software controls
- Network controls
- Environmental controls
- Small installations

Introduction

1. General controls are those that are not specific to individual applications but that affect the entire processing environment in which the applications run.

Risk

2. The reliability of financial information produced from computer applications depends upon the adequacy of the controls over the processing environment as well as those over individual applications. Put more simply, it is no good running secure and reliable applications in an unsound processing environment.

Overall audit objectives

3. The overall audit objectives of a data centre review are " ... to ensure that the controls and procedures governing the organisation of staff, operational functions, access to files and software and general environmental protection, provide safe and efficient day to day operation of the computer installation." (CIPFA).

Areas of audit interest

4. The following control areas should be examined:

- Planning for the information systems department
- Organisational controls
- Operational controls
- Files & software controls
- Environmental controls
- Network controls
- Terminal (often users and separate but included)

For each of the above areas some typical control issues/audit checklists are mentioned in the following sections:

Typical control issues

Planning for the information systems department

5. Audit objectives: To ensure that senior management is sufficiently involved and that the

information systems department's long and short-term plans are integrated into the organisation's overall plans.

6. Audit Scope: Controls and procedures for the IT planning process.

7. Typical control issues:
   - Is senior management involved fully in the planning process?
   - Are the long and short-term goals of the organisation identifiable?
   - Are long and short-term IT goals compatible with the organisations overall goals?
   - Is there an IT Planning/Steering Committee with agreed terms of reference?
   - Are major users represented on the Committee?
   - Are the Committee's goals consistent with the organisation's goals?
   - Is the Committee achieving its goals?

Organisational controls and personnel issues

8. Audit objectives: To ensure that there is an adequate separation of duties and comprehensive written standards, policies and procedures.

9. Scope: Controls and procedures over the organisation of the responsibilities of those involved and the standards established for their efficient working.

10. Typical Control issues:

    a) Personnel procedures:

   - Do personnel selection criteria include education, experience, attendance and responsibility?
   - Is personnel security clearance obtained before employment, where applicable?
   - Is employee job performance evaluated regularly against established criteria?
   - Upon suspension or termination for disciplinary reasons are personnel:
     - ○ Paid in lieu of any termination period
     - ○ Required to relinquish all passes/keys providing access to computer facilities
     - ○ Escorted immediately from the premises to avoid damage to computer facilities or data?
   - Does training planning and provision for IT reflect the strategic aims of the IT ?

b) Allocation of responsibilities/segregation of duties:

Allocation of responsibilities:

- Can the major units of the IT Department be identified from documentation?
- Is there a clear chain of command?
- Is the allocation of duties between users and the IT function clearly defined?
- Are there written job descriptions for all IT department positions that clearly describe their authority and responsibilities?
- Does the job description of an officer include the role of security officer?
- Does the IT Department have sufficient organisational independence from user departments?
- Are the relative responsibilities of the IT department and users clear, documented, appropriate and complied with?
- Are users responsible for initiating transactions and checking their completeness and accuracy at all stages?
- Where online data entry has been devolved to users, are the controls operated by them as tight as would be operated by a central computer control section?
- Is there a clear allocation of duties?

Segregation of duties:

- Does documentation show a segregation of duties between:
  - ○ Systems development and operations?
  - ○ Operations and data control?
  - ○ Database administration and systems development?
- Is the intended segregation of duties being maintained?
- Are the duties of personnel working in sensitive areas rotated?

c) Standards:

Are there standards covering the entire range of IT activities including:

- Operating procedures
- Standby facilities
- Personnel recruitment and vetting
- Training
- File access
- Care and maintenance of hardware
- Procedures for developing new systems including by users
- Documentation for software and data files
- Network and terminal connections.

Operational controls

11. Audit objectives: To ensure that there is adequate discipline and uniformity for all aspects of day to day running of production systems.

12. Scope: Controls and procedures relating to data preparation and the control of data during processing.

13. Typical control issues:

a) Controls over the receipt and conversion of data

Are there procedures to ensure that:

- Prime data is authenticated?
- The movement of sources of input (e.g. bills) is controlled?
- Input data is validated for accuracy?
- Input data is correctly converted to machine-readable form?

b) Control of data during processing

- Are there controls to ensure that only the correct data and programmes are processed?
- Are there job schedules for all data processing?
- Is operator training adequate?

c) Controls over distribution of output

- Are schedules maintained of the output from applications and their recipients?
- Do controls ensure that output is:
  - -Timely?
  - -Accurate?
  - -Relevant?
  - -Not excessive?
  - -Received by the correct recipients?
  - -Secure?

d) Operating system controls

- Does the operating system adequately restrict access to files?

- Are there written authorisations from users for changes to access rights to their data? (NB: Audit is entitled to read only access to all systems but should request permission from the system owner as a courtesy)
- Are there written guidelines for password changes?
- Is there adequate provision for file backup and standby?
- Are the facilities for gathering and recording information on job runs activated?
- Are the selected operating system options documented?
- Is machine usage analysed by job, user system etc?
- Is machine performance monitored regularly?

e) Recovery controls

- In case of processing failure, are operators trained in recovery procedures?
- Are recovery procedures:
  - Efficient?
  - Designed to start re-processing from the last correct record?
  - Documented for all financial applications?
  - Tested?

File and software control

14. Audit objectives: To ensure that controls and procedures adequately safeguard data files and software against all forms of loss, unauthorised disclosure and provide for the recovery of information lost.

15. Scope: Controls and procedures governing the access to and protection of all physical magnetic files and their contents.

16. Typical control issues:

a) Controls over physical file custody

- Are there adequate controls over:
  - The security of file storage?
  - Issue and return procedures?
  - File maintenance?
  - Logical storage?
  - Retention?

- Remote storage, logical ownership?
- Different generations?

b) Controls over access to software

- Is all software held securely?
- Are only authorised personnel able to access software?

c) File identification, systems software, modes of access and file encryption

- Is there a systematic procedure for labelling files?
- Are all files clearly labelled?
- Are files encrypted as necessary (e.g. password files)?

d) Controls over programme changes

- Do all programme changes require:
    - Written authorisation?
    - Documentation standards?
    - Independent testing?
    - Authorisation before an amended programme is used in a live environment?

e) Back-up

- Are there regular back-ups of data, application and system files?
- Do back-ups cover a sufficient period?
- Do labelling and storage arrangements provide control over different generations of back-up file?
- Are back-up files stored securely in a separate site?
- For minor processing interruptions are there:
    - Written restore procedures for each application?
    - Alternative processing arrangements?

Network controls

17. Audit objectives: To ensure that all terminal and network activity is properly authorised, and that inaccurate and inefficient processing is minimised.

18. Scope: Those governing the access to and processing performed by all terminals connected to the computer installation.

19. Typical control issues:

a) Administrative access controls

- Are there written administrative guidelines covering:
  - Those authorised to access computing facilities?
  - The acceptable use of different access types (cable, network, dial up etc)?
  - The set up, change and termination of usernames?
  - Password set-up and changes?
  - Data security?

b) Physical restrictions on access

- Are machines located in secure areas and accessible only to authorised personnel?

c) Software restrictions on access

- Does software provide adequate restrictions on access?

d) Recording terminal activity

- Is terminal activity controlled and monitored?

Environmental controls

20. Audit objectives: To ensure that there is adequate protection for the staff, computer equipment and environment, software, data and documentation against deliberate or accidental damage and to ensure continuity of service in the event of a major disaster.

21. Scope: Controls and procedures to avoid the risk of major processing interruptions and those designed to recover from major disasters.

22. Typical control issues:

a) Protection against threats

- Has data been classified in terms of the following types of loss:

  - Direct financial?
  - Indirect financial?
  - Loss of control over the organisation's activities?
  - Embarrassment to the organisation?

- Is potential loss from accidents minimised:

  - Natural disasters e.g. cyclones etc?
  - Fire and smoke?
  - Flood or ingress of water?
  - Power fluctuations?
  - Disruption of essential services?

- Is possible loss from deliberate sources acts minimised:

  - Vandalism and sabotage?
  - Theft?
  - Fraud?
  - Unauthorised use?

b) Continuity of operation

- Is the priority to be given to applications pre-defined?
- In case of temporary processing unavailability is there a reciprocal agreement to provide alternative facilities?
- In case of a major processing disaster is there:
  - A written disaster contingency plan?
  - Evidence of testing of the contingency plan?

Small installations

23. The audit issues for a small installation are similar to those for a major data centre and many of the typical control issues above will apply. However, fewer staff are likely to be involved and there may well be less opportunity to impose an adequate division of duties. The IT auditor may therefore need to place greater reliance upon existence of supervisory and monitoring controls.

PART C3

Procurement of IT facilities

This section deals with the following:

- Introduction
- Role of the IS auditor
- Risks
- Audit objectives
- Typical control issues

Introduction

1. The procurement of IT embraces the full range of IT related facilities - equipment, software, networking infrastructure, services such as facilities management, and related issues such as financing, insurance and compliance with legislation.

Role of the IS auditor

2. Audit should determine:

- Whether or not the management arrangements and procedures for procurement will meet the objectives of management;
- Whether the arrangements and procedures have been applied in practice.

Risks

3. The risks of inadequate controls over the procurement of IT assets include:

- Wrong equipment acquired;
- Business needs not satisfied;
- Budgetary control undermined;
- Legal responsibilities not met;
- Excessive cost;
- Implementation delays.

Audit objectives

4. These are to ensure that:

- IT procurements are consistent with the organisation's business and IT strategy;
- Procurement conforms to procurement regulations and to any legal requirements;
- Methods of financing are appropriate for the facilities being acquired;
- The method for selecting the successful tender is sound;
- The installation and implementation of the procurement is effectively managed;
- Post-implementation reviews are carried out to ensure that the objectives of the procurement have been met.

Typical Control Issues

CONTROL	ANSWER		COMMENTS	W/P REF
	Y	N		
Is there an overall group responsible for reviewing IT procurements appropriate to the organisation's IS/IT strategy?				
Do guidelines exist to assist in the procurement process?				
Has the organisation appropriate knowledge of and expertise in the relevant Government requirements, rules and regulations?				
Does the procurement adhere to Government requirements, rules and regulations on threshold values, estimates and aggregation rules?				
Does the procurement comply with to Government requirements, rules and regulations relating to procurement processes including publishing notices, selecting suppliers, and awarding contracts?				
Do technical specifications and references to standards in the requirements specification conform to Government requirements, rules and regulations?				
Have methods of financing been investigated?				
Is the method chosen sound and in line with the organisation's overall financial strategy?				
Is appropriate approval given to the method chosen?				
Is the method of tender evaluation approved and consistent with the criteria for award of contract specified within contents of any published notice?				
Does the proposal meet the technical requirements of the specification?				
Is a business appraisal undertaken?				
Is the method of tender comparison sound?				
Is a contract appraisal undertaken?				
Is a recommendation and decision made based on the evaluation of the tenders?				
Is an installation/implementation programme planned?				
Are facilities tested prior to acceptance?				
Are appropriate resources available to achieve the implementation plan?				
Are post-implementation reviews undertaken within agreed timescales?				

PART C4
Reviewing existing computer applications

This section deals with the following:

- Introduction
- Audit risks
- Role of the IT auditors
- Audit objectives
- Typical control issues

Introduction

1. The stages in reviewing a computer application are:

- Document the system
- Carry out 'walk through tests' to confirm understanding of system controls
- Evaluate the strengths and weaknesses of the controls.

2. The conclusions reached form the input to designing the audit testing approach.

Audit risks

3. These include:

- lnsufficient appreciation of the need for and less capacity to apply basic controls such as validation checks within applications.
- Inadequate control over the input, processing and output of data.
- The possibility of individual users being responsible for development and maintenance of systems, as well as input of data and operations.
- The development of systems using spreadsheets and database packages which may not allow for the expected level of controls to be included.
- Systems developed by an individual for their own use may come to be used for much wider corporate purposes without the necessary controls being built in.
- Where data is input online the availability or batching of documents and provision of input control totals is likely to have decreased and this may, in turn, remove evidence of an audit trail or at least require additional controls to maintain the audit trail.

The role of the IT auditor

4. With the possibility of lowered standards of controls within applications there is a much greater need for the auditor to consider the relationships between controls within the application, administrative controls around it and general computer controls within the organisation. These areas are likely to overlap and the auditor should be satisfied as to the adequacy of general controls before assessing controls within the application.

Audit objectives

5. These include:

- Each transaction is authorised, complete, accurate, timely and input once only.

- An appropriate level of control is maintained during processing to ensure completeness and accuracy of data.
- Controls ensure the accuracy, completeness, confidentiality and timeliness of output reports and interfaces.
- A complete audit trail is maintained which allows an item to be traced from input through to its final resting place, and a final result broken down into its constituent parts.
- Arrangements exist for creating back-up copies of data and programmes, storing and retaining them securely, and recovering applications in the event of failure.

Typical control issues

CONTROL	Y	N	COMMENTS	W/P REF
Are transactions from recognised sources?				
Is control established over transactions at the earliest opportunity?				
Are transactions explicitly authorised by either manual or electronic means?				
Are password controls effective in restricting access?				
Are input and authorisation functions restricted and separated?				
Is input of parameters for processing and other standing data strictly controlled?				
Is data subject to validation for completeness and accuracy at input stage?				
Are there clear procedures for data items rejected on input?				
Do clear timetables exist for input and are they adhered to?				
Are checks made to detect possible duplicate input records?				
Does a clear processing schedule exist and is it understood by users and operations staff?				
Is all data, including that transferred from other systems, subject to appropriate validation during processing?				
Is data processed by the correct programmes and written to the correct files?				
Do programmes provide confirmation that processing has been completed successfully, or do recovery and resubmission procedures exist to deal with abnormal terminations?				
Is assurance provided that all records have been processed?				
Do procedures exist for handling records rejected by application programmes?				

CONTROL	Y	N	COMMENTS	W/P REF
Are staff responsible for handling output, carrying out checks to ensure its completeness and reasonableness?				
Is output identified and does it include information that demonstrates completeness?				
Do arrangements for the distribution of output procedures ensure that it goes to the correct location/users and that confidentiality is maintained?				
Is the usefulness of output kept under review?				
Is confidential output disposed of securely?				
Is unique source information retained for all transactions?				
Are input documents and output reports filed in such a way as to facilitate tracing transactions through the system?				
Can totals on control reports be broken down into the transactions that form the totals?				
When records are posted from one financial system to another, are those input to the second agreed with those output by the first?				
When records are rejected when transferred between systems, can they be identified and investigated?				
Are the users responsible for input, amendment or deletion of transactions recorded within the system?				
Where audit trail reports are provided, are they complete, and do journals indicate if and when trail mechanisms are switched off?				
Are files backed up at intervals during processing to allow recovery of jobs?				
Are audit trail reports provided where needed?				

PART C5

Major enhancements and new applications under development

This section deals with the following:

- Introduction
- Audit risks
- The role of the IT auditors
- Audit objectives
- IS maintainence practices & typical Audit Tasks

Introduction

1. This section deals with the audit issues arising when an IT auditor reviews the development of a new information system or major changes to an existing system.

Audit risks

2. There are considerable risks associated with such IT development including:

- Failure to provide the desired functionality;
- Insufficient skilled resources;
- Wastage of valuable development resources;
- Lack of control within new applications or a reduction in the level of internal controls as the result of an enhancement.

The role of the IT auditor

3. The role of the IT auditor is to assess the risks at each stage of development and to make recommendations to reduce those risks. The classic phases of the development/acquisition of a new computer application and the role played by the IT auditor is illustrated in the following table:

Information System Development Phase	**Typical Areas of Audit Review**
Project Management	· Organisational project management standards are followed.
Requirements definition	· Major requirements are identified; · User needs are specified; · Audit (e.g. reporting and audit trail) requirements specified.
Feasibility study	· Business case is made; · Need for computerisation justified; · Major variables identified (e.g. time frame); · Availability of vendor products assessed; · Approximate cost identified; · Case for external or internal acquisition documented.
Software acquisition	· IT Procurement rules followed for external acquisition; · Development standards applied for internal acquisition.

Information System Development Phase	**Typical Areas of Audit Review**
Detailed design	· Preliminary screens designed; · Preliminary tests; · User requirements refined; · Data flows documented; · Controls documented; · Preliminary data conversion plans written.
Programming	· Modifications made to externally acquired software; · In-house routines written; · Conversion routines written and tested.
Testing	· Separate test environment created; · System testing carried out; · Entire system not just individual programmes examined; · Hardware capacity stress tests completed; · Pilot/parallel running.
Implementation	· Data conversion plan implemented including controls; · User procedures written; · Technical and user and training completed; · System migration completed.
Post-Implementation Review	· System adequacy assessed; · Cost/benefits realised; · Correction of deficiencies planned.

4. The IT auditor must be careful to provide added value to the organisation whilst retaining independence. This is not easy in practice. On the one hand it is vital that audit input is made during the course of development, otherwise essential controls may be missed. Furthermore, once an information system is implemented it is often too costly and time-consuming to build in important controls. The result may be lack of preventative controls and/or relatively high costs in the form of administrative manual controls that could have been avoided. On the other hand, the Auditor must not sacrifice his/her ability to maintain independence from the management decisions that form part of any development. Compromise of that independence may restrict the Auditor's ability to comment objectively on the system in the future.

5. The IT auditor will need to construct a controls matrix that can be completed at the appropriate point in the implementation to maintain a balanced view of the control status of the development.

Audit objective

6. The IT auditor's main objective is to ensure that controls within the system under development will be adequate once it has been implemented. The key control objectives with which the auditor will be concerned are in many respects similar (e.g. completeness of input etc.). However, there is clearly the additional dimension the development/acquisition process to consider.

IS Maintenance Practices and Typical audit tasks

7. The main tasks of the IT Auditor include the following :

- Evaluate systems maintenance standards and procedures;
- Test system maintenance procedures for compliance;
- Evaluate the maintenance process to see that it is achiveving its objectives;
- Determine the quality of production library security;
- Assess change control procedures for adequacy.

CONTROL	Y	N	COMMENTS	W/P REF
Do projects comply with the IS/IT strategy and respond to business needs?				
Have project development standards and pollcies been defined and adopted?				
Does an IS/IT strategy team review and approve projects?				
Is a project management team appointed?				
Is a project manager appointed for each project?				
Is there a business case compiled by the budget holder/user and does it reflect all direct and indirect costs and benefits?				
Is a comprehensive feasibility study prepared for approval?				
Is a project plan agreed by the budget holder/user and developer/provider?				
Do structured procedures exist for small-scale projects?				
Is financial control exercised throughout the project?				
Does the project have appropriate approval to proceed?				
Does the selection of the developer/provider comply with sound tendering practice?				
Is a contract or service level agreement agreed between the budgetholder and developer/provider?				
Do all parties know of and comply with all legal obligations?				
Does project design reflect the optimum use of available technology and techniques and security and control considerations?				
Are installation, testing and acceptance agreed by the user and provider?				
Is documentation developed to the agreed standard and delivered within the agreed timescale?				
Are staff properly trained in the system?				
Is a post-implementation review undertaken within an agreed period?				

PART C6

Data conversion reviews

This section deals with the following:

- Introduction
- The main steps in IT conversions
- Audit risks
- Audit objectives
- Typical control issues

Introduction

1. A conversion is a transfer of data from one storage medium to another. When a manual system is computerised data is converted from card systems and manual ledgers etc to computer files. Likewise, when a computer application is replaced it is often necessary to convert the data file so that the new system can read it.

The main steps in IT conversions

2. Although not always in this strict order, an IT conversion usually includes:

- Installation of hardware
- Creation and validation of the initial data source
- Conversion of the master and transaction files
- Reconciliation of the old and new files
- Parallel running
- Comparison of the output from the old and new systems
- Formal user acceptance of the new system
- Formal user approval to cease using the old system.

Audit risks

3. Conversions pose a number of potential risks for auditors. They are one-off exercises with significant implications for the reliability of financial records but they are often carried out in an unstable environment brought about by unfamiliarity with the new system and with the conversion process itself, new technical problems and changes in the control regime etc.

4. Potential data errors include incorrect opening balances, incorrect or incomplete master and transactions file data, incorrect cut-offs for transactions data and the introduction of unauthorised transactions. Errors may also arise from changes to accounting procedures and internal controls including authorisationl supervisory changes, new forms/input measures, new control reports etc. There may also be changes to accounting policies. The auditor will need to review these to ensure that they are appropriate, allow identification, quantification and proper disclosure. Contingency arrangements also are required in case of system failure.

Audit objectives

5. These are to:

- Assess the audit risk associated with the conversion including the adequacy of controls and compliance with them;
- Carry out audit testing as required;
- Identify management letter points;
- Assess whether specialist IT audit help is required;
- Assess the potential for present or future CAATs use.

Typical control issues

6. There should be:

- A written conversion plan containing all of the tests to be performed by the users performing the tests, the expected results and space for a comparison with the actual figures;
- Evidence of old and new data reconciliation;
- Evidence of user involvement including formal user acceptance of the converted data;
- Evidence that programme change procedures have been followed;
- Compliance tests carried out by the IT auditor to ensure that the conversion plan has been followed;
- Substantive testing carried out by the IT auditor on balances and other master file data;
- A review of conversion results by the IT auditor to confirm the correct use of authorisations, reconciliations, comparisons with parallel run output and reviews of pilot test data etc.

PART D

Using Computer Assisted Audit Techniques (CAATs) and Tools

This section deals with the following:

- Introduction
- Audit testing and Computer Assisted Audit Techniques (CAATs) and tools
- Advantages of CAATs
- Main types and uses of CAATs
- When to use CAATs
- Data extraction and manipulation software
- How IDEA can be used
- Test data

Appendix D.1: Examples of audit tests using data extraction and manupulation software

Introduction

1. Computer Assisted Audit Techniques (CAATs) and tools include all instances where a computer is used to assist in the performance of audit procedures. CAATs may be used both to test the operation of internal controls within a system as well as to perform transaction testing to support an audit opinion on a set of accounts. Using CAATs it is often possible to test 100% of transactions in less time than is required to test a small sample manually thus raising both the quality and efficiency of financial audit work whilst at the same time raising assurance levels.

Audit Testing and Computer Assisted Audit Techniques (CAATs)

2. Where information gathering indicates that controls are strong, compliance tests can be conducted using a relatively small sample from each transaction type. Weak controls should be tested substantively to identify incorrect data resulting from the inadequacies. In some cases e.g. the transfer of balances between systems some substantive testing will always be required.

3. Audit tests provide reasonable assurance that there has been no material error; they do not guarantee the total absence of error. Professional judgment is required to gauge the nature, extent and timing of audit tests.

4. Audit tests should be designed by starting from a management assertion (e.g.Existence). This provides the audit objective (e.g. To confirm the existence of.. ..) which in turn translates into an audit procedure (e.g. Interrogate the transactions file to confirm the existence of.. ..). Compliance tests check that internal controls are working properly. Substantive tests confirm that processed data is valid.

5. Information systems pose a number of special problems when designing and carrying out audit tests (e.g. controls are often internalised). This can be overcome by using IT Audit Assisted Techniques.

Advantages of CAATs

6. The main advantages of CAATs are that they:

- Provide comprehensive audit coverage
- May be the only feasible testing method
- May be the most cost effective method
- Permit new audit tests

- Eliminate tedious work
- Increase credibility with clients.

Main types and uses of CAATs

7. CAATs generally fall into two categories, namely:

- CAATs used for reviewing data, and
- CAATs used for reviewing programme controls.

8. CAATs for reviewing data involve examination of files containing standing and transaction data, system journals, recovery logs or data communication logs. The CAATs often used for reviewing file data are:

- Data extraction and manipulation software (see below)
- Embedded audit modules.

9. CAATs for verifying the operation of programmes/systems procedures and controls are used to test the effectiveness of programmed routines or controls operating within systems to judge the reliability of their operation. Relevant techniques are:

- Test data (see below)
- Integrated Test Facilities
- Parallel Simulation
- Programme review or code analysis.

10. In practice, file interrogation techniques are the most frequently used computer assisted audit techniques and can be used for testing both data and the operation of system controls.

When to use CAATs

11. The use of CAATs is not appropriate to all circumstances. They should be considered where there is:

- A core purpose or reason
- A reasonable number of records
- A depth of information about the records
- Accessible data.

Data extraction and manipulation software

12. Data extraction and manipulation software is the most popular form of file interrogation technique and therefore the most popular CAATs. This type of software comprises a computer programme or series of programmes designed to perform file interrogation and analysis tasks:

- Examine records based on specified criteria
- Testing calculations and making computations
- Comparing data on separate files
- Selecting and printing audit samples
- Summarising or re-sequencing data and performing analyses
- Comparing data obtained from other procedures with computer records.

13. An example of a file interrogation facility is the Interactive Data Extraction and Analysis (IDEA) software.

How IDEA can be used

14. For routine audits IDEA can be used to meet the following objectives:

Audit objective	Examples of relevant IDEA procedures
Mechanical Accuracy	· Field Statistics function to add fields. · Append or Virtual Fields options to check calculations.
Analytical review	· File stratification to profile data by value bands, codes or dates .
Validity (exception tests, compares and duplicates)	· Exception tests for relationships between items of data or allowable values. · Statistical sampling. · Duplicates testing.
Completeness (gaps and matches)	· Gap Detection to identify missing sequential numbers. · Transactions file to master file checking.
Correct cut-off	· Exception tests for items with dates outside the required cut-off.
Other audit objectives	· Production of 'views' of data to provide information on e.g. provisions or valuations.

15. The attached Appendix E.I contains examples of audit tests that can be carried out on the main financial ledgers and data using data extraction and manipulation software.

16. Steps in the use of file interrogation software for testing are:

Step 1: Define the audit objective;

Step 2: Obtain information about the file and record layout, availability, and security;

Step 3: Check client's hardware/data is compatible with audit software;

Step 4: Define subsequent procedures, required calculations, logic, reports and application controls;

Step 5: Develop coding or logic instructions;

Step 6: Test and review results;

Step 7: Process against required file;

Step 8: Review results and compare with control totals.

Test data

17. This is another popular CAAT. Its main use is to verify the operation of system procedures and controls. Test data can be used for:

- Verifying input edit checks using invalid data;
- Checking complex programme calculations;
- Verifying control totals and balancing routines;
- Checking the accuracy of internally generated transactions;
- Confirming understanding of the system.

18. The usual audit test conditions for inclusion are:

- Tests for invalid conditions;
- Duplications;
- Out of limit conditions (e.g. payments in excess of pre-defined limits);
- Incomplete, invalid or missing input;
- Wrong master file or transactions file;

- Format test for important fields;
- Illogical conditions (e.g. payment date prior to data input date).

19. Steps in testing are:

Step 1: Define the audit objectives;

Step 2: Prepare test transactions from:

- previously processed transactions
- programmer's original test data
- conditions to be tested.

Step 3: Determine the expected results;

Step 4: Compare processed with expected results.

Appendix D.1

Examples of audit tests using data extraction and manipulation software

General Ledger

1) Calculation:
   - Cost (total) the balances to ensure they balance to zero (some memo accounts may need to be excluded.
   - Total (or summarise) transactions by account to prove the trial balance.
   - Re-perform automatic allocations over accounts.
   - Re-perform account summarisation for management accounts, financial accounts or consolidation.

2) Analysis:
   - Compare balances with previous periods, budgets or management accounts to show variances and fluctuations.
   - Provide totals of entries generated by different sources (e.g. purchase or sales ledger, journal vouchers, etc.) to show the volume and value.

3) Exception tests:
   - Test for transactions with dates outside the posting month or year (cut-off).
   - Test for duplicate postings.
   - Provide detailed analysis of selected accounts.

4) Sampling:
   - Provide samples of postings for verification (the sample could be random, exception-based or specified entries).

Payroll

1) Validity of employees on payroll.

2) Pay entitlement
   - Calculation of gross pay
   - Calculation of deductions
   - Calculation of net pay.

3) Costing and Sampling.

4) Duplication.

5) Reasonableness of
   - Tax details
   - Pay/grade comparison
   - Hours worked
   - Holiday taken
   - Date joined
   - Date of birth (e.g. over 16 and within age range for employment).

6) Comparison of payroll files at two dates to determine recorded starters and leavers and change in pay etc.

7) Comparison of list of employees on payroll, over retirement age, and on pension file.

Sales ledger

1) Identifying credit balances
2) Analysing transaction by age
3) Perusing movements on selected accounts
4) Looking for invalid transaction types
5) Looking for excess over limits placed on accounts
6) Identifying any credits in accounts
7) Identifying accounts with no movements during a certain period
8) Casting the file
9) Selecting samples for testing
10) Identifying part payment of debts
11) Ensuring correction of balances on selected accounts
12) Testing for cut off.

Accounts payable

1) Comparing files at two dates and identifying new suppliers.
2) Validity of suppliers.
3) Testing for duplicate payments.

Identifying debit balances

1) Providing samples for testing purposes
2) Testing cut-off
3) Identifying old invoices
4) Identifying unusual data
5) Checking on regularity of payments (e.g. loss of discounts).

ABBREVIATIONS

ASOSAI	Asian Organization of Supreme Audit Institutions
CAAT	Computer Assisted Audit Techniques
CIPFA	The Chartered Institute of Public Finance & Accountancy
DG	Director General
FMRP	Financial Management Reforms Programme
IDEA	Interactive Data Extraction and Analysis
IFAC	International Federation of Accountants
INTOSAI	International Organization of Supreme Audit Institutions
ISSAIs	International Standards of Supreme Audit Institutions
ISACA	Information Systems Control and Audit Association
IS	Information System
IT	Information Technology
MIS	Management Information System
OCAG	Office of the Comptroller and Auditor General
SAI	Supreme Audit Institution