# Table of Contents

1. **INTRODUCTION** .......................................................................................................................... 1  
   1.1 Aims and objectives .................................................................................................................. 1

2. **IT AUDIT STANDARDS** ............................................................................................................ 1  
   2.1 Introduction ............................................................................................................................. 1
   2.2 International Standards ........................................................................................................... 2
   2.3 National Standards .................................................................................................................. 4
   2.4 Individual Organisations ......................................................................................................... 4
   2.5 Professional Bodies ................................................................................................................ 4
   2.6 Other Bodies .......................................................................................................................... 8

3. **ORGANISING IT AUDIT** ....................................................................................................... 9  
   3.1 Introduction ............................................................................................................................ 9
   3.2 Relevant Skills ....................................................................................................................... 9
   3.3 Acquiring Skills ..................................................................................................................... 11
   3.4 Selection of Specialist Auditors ........................................................................................... 11
   3.5 Organisation of IT Audit Function ......................................................................................... 11
   3.6 Scheduling Audit Resources ............................................................................................... 12
   3.7 Assessing priorities ................................................................................................................ 13
   3.8 Planning .................................................................................................................................. 17

4. **TRAINING AND AWARENESS** ............................................................................................. 20  
   4.1 Training Strategy .................................................................................................................... 20
   4.2 IT Audit Training .................................................................................................................... 20
   4.3 Qualifications ........................................................................................................................ 21
   4.4 Training Logs .......................................................................................................................... 21
   4.5 Technical Library .................................................................................................................... 21
5. CONTINUING PROFESSIONAL EDUCATION ......................................................... 23

5.1 Professional Qualifications ................................................................................. 23
5.2 Workshops, seminars and other forms of CPE ...................................................... 23

6. MONITORING AUDITEE DEVELOPMENTS ..................................................... 24

6.1 Understanding an auditee, Operations and IT Organisation ..................................... 24
6.2 Sources of Information ......................................................................................... 25
6.3 General Review of IT ............................................................................................. 25
6.4 IT Legislation and Regulation ............................................................................... 26
6.5 Documentation ...................................................................................................... 26

7. EXTERNAL CONSULTANTS .............................................................................. 27

7.1 Introduction .......................................................................................................... 27
7.2 Why Use Consultants? ........................................................................................... 27
7.3 What Kind of Consultant? ....................................................................................... 28
7.4 Notifying the Auditee ............................................................................................. 29
7.5 Short-listing Candidates ......................................................................................... 29
7.6 Financial Control ................................................................................................... 30
7.7 Seeking Bids .......................................................................................................... 30
7.8 Assessing Proposals ............................................................................................... 31
7.9 Working Relationships ......................................................................................... 31
7.10 Managing the Work ............................................................................................. 32
7.11 Reviewing Findings ............................................................................................. 32
7.12 Consultants’ Reports ............................................................................................ 33
7.13 Assessing Performance and Learning Lessons ...................................................... 33
8. IT AUDIT APPROACHES ................................................................. 35

  8.1 Why and When to Use an IT Auditor ................................................. 35

  8.2 INTOSAI IT Audit Curriculum ...................................................... 38

  8.3 Identification of Material Risk Areas ............................................. 38

  8.4 Using Computer Assisted Audit Techniques ................................... 40

9. QUALITY ASSURANCE ............................................................... 43

  9.1 Supervision and Quality Assurance ................................................ 43

  9.2 First Stage Review ............................................................... 43

  9.3 Second Stage Review ............................................................ 44

  9.4 Quality Control Review .......................................................... 44

  9.5 Communication with Auditees ...................................................... 45
1. INTRODUCTION

1.1 Aims and objectives
This module deals with fundamental aspects of organising and managing an IT audit. Its aim is to provide an awareness of the correct professional approach to IT audit that will help to ensure objectives are met. We will cover the following topics:

- IT audit standards;
- organising IT audit;
- training and awareness;
- continuing professional education;
- monitoring auditee developments;
- external consultants;
- IT audit approaches; and
- quality assurance.

We should emphasise at the outset that the review of an auditee’s IT systems is likely to form just one part of a wider audit - whether a financial audit or a value for money audit. The presence of IT does not alter the fundamental audit objectives. The IT auditor should therefore support the general auditor in the fulfilment of those objectives.

2. IT AUDIT STANDARDS

2.1 Introduction
There are typically four levels of auditing standards which may influence the audit practices and methodologies within individual SAIs:

- at the highest level there are INTOSAI’s own standards in government auditing, as well as the international auditing standards promulgated for the private sector by the International Auditing Practices Committee of the International Federation of Accountants (IFAC);
- at the next level, the national auditing standards body of each country develops its own standards;
- then there are the auditing standards of the individual SAIs and other auditing bodies in each country; and, finally, there are
- standards are set by professional organisations such as the Information Systems Audit and Control Foundation (ISACF) to which individual auditors may belong.

Both international and national auditing standards tend to be aimed exclusively at the audit of financial statements. Standards relating to value for money audit are usually found at an organisation level, together with standards relating to the audit of financial statements.
Organisations may set their own standards for their internal auditors. External auditors should assess the appropriateness and adequacy of such standards, and the extent of the internal auditor’s adherence to them, before placing any reliance on the work of internal auditors.

2.2 International Standards

INTOSAI

While INTOSAI Auditing Standards do not have mandatory application, they reflect a “best practices” consensus among SAIs. Each SAI must judge the extent to which the standards are compatible with the achievement of its mandate. The INTOSAI auditing standards in government auditing consist of four parts - basic postulates, general standards, field standards and reporting standards.

Paragraphs 18 and 19 of the INTOSAI standards state:

“The SAI must judge the extent to which external auditing standards are compatible with the SAI’s fulfilment of its mandate. The SAI should recognise, however, that the INTOSAI auditing standards embody a consensus of opinion among government auditors and try to apply them where they are compatible with the SAI’s mandate. The SAI should seek removal of incompatibilities where this is necessary to permit the adoption of desirable standards.

For some elements of the SAI’s mandate, particularly in regard to the audit of financial statements, the SAI’s audit objectives may be akin to the objectives of audits in the private sector. Correspondingly, the private sector standards for financial statements auditing which are promulgated by official regulatory bodies might be applicable to the government auditor.”

This indicates that, to all practical intents and purposes, the standards that will be applied by an SAI to the audit of financial statements will be those standards promulgated by such organisations as the International Federation of Accountants for audits in the private sector.

Whilst there are no specific INTOSAI standards that address audit in a computer environment, the field standards on planning, supervision and review, the study and evaluation of internal control, and audit evidence apply as much to audits in a computer environment as they do to all other audits.

International Federation of Accountants (IFAC) Standards

The International Federation of Accountants (IFAC) is a federation of those national accounting bodies recognised by law or general consensus within their countries as substantial national organisations of good standing within the accountancy profession. It aims to improve the harmonisation of auditing practices throughout the world. Whilst auditors should comply with the national standards of their own country, these should usually match those set by IFAC. Where they differ, auditors should ensure that they comply with the more stringent standard.

The overall objective and scope of an audit do not change with the introduction of a computer information system environment, but the use of a computer will change the processing, storage and communication of financial information and may affect the accounting and internal control systems employed by the entity. The following are examples of relevant international standards on auditing (ISAs) that will apply to all audits we carry out irrespective of whether the auditee uses manual or computerised systems.
ISA 200  “Objective and General Principles Governing an Audit of Financial Statements”
ISA 220  “Quality Control for Audit Work”
ISA 300  “Planning”
ISA 310  “Knowledge of the Business”
ISA 400  “Risk Assessments and Internal Control”
ISA 620  “Using the Work of an Expert”

IFAC has, however, established additional standards with specific relevance to auditing in a computer information systems environment:

ISA 401  “Auditing in a Computer Information Systems Environment”

This establishes standards and provides guidance on procedures to be followed when an audit is conducted in a computer information system environment. Such an environment exists when a computer of any type or size is involved in the processing by an entity of financial information of significance to the audit, whether that computer is operated by the entity or by a third party.

ISA 401 sets out considerations for the auditor in determining how a computer information system environment will affect the audit and therefore the audit plan. As the ISA makes clear, a computer information system environment will affect:

• the procedures the auditor will follow in obtaining a sufficient understanding of the accounting and internal control systems;
• the consideration of inherent risk and control risk in determining the risk assessment; and
• the design and performance of tests of control and substantive procedures appropriate to meet the audit objective.

The Standard maintains that a sufficient level of skills and competence must be employed in the audit of a computer information system environment.

ISA 1008  “Risk Assessments and Internal Control - EDP Characteristics and Considerations.” [Addendum 1 to the ISA on Risk Assessments and Internal Control]

This Standard sets out specific characteristics of a computer information system environment in respect of organisational structure, nature of processing, design and procedural aspects and internal controls (comprising general controls, application controls and control review) to be considered in the assessment of risk in planning an audit.

ISA 1009  “Computer-assisted Audit Techniques”

This Standard provides guidelines in the use of CAATs, and applies to all uses of CAATs involving a computer of any type or size.

International Federation of Accountants (IFAC) Statements

Furthermore, three statements have been issued by IFAC which are intended to provide the auditor with guidance in implementing these Standards, but do not have the authority of an ISA. They are:
• Statement 1001, EDP Environments - Stand-alone Microcomputers;
• Statement 1002, EDP Environments - On-line Computer Systems; and
• Statement 1003, EDP Environments - Database Systems.

2.3 National Standards

Most countries have established an auditing standards body responsible for setting standards at a national level. The basic principles and essential procedures set by these standards tend to be consistent, more or less, with the International Standards set by IFAC; national standards exist to allow for variations due to local circumstances.

Recent developments in the UK auditing profession have resulted in the issue of new Statements of Auditing Standards (SASs). However, the Auditing Practices Board in the UK has only issued guidelines on auditing in a computer information systems environment and on the use of CAATs, without giving them the force of a standard. This is not the case in all countries. In Australia, for example, Auditing Standard AUS 214 “Auditing in a CIS Environment” is consistent in all material respects with ISA 401 and has the force of a standard.

2.4 Individual Organisations

National Supreme Audit Institutions

A SAI usually establishes explicit auditing standards to govern its work. These encapsulate the key factors which underpin the quality of that work. For example, the UK NAO’s overall policy is to comply in all respects with the standards issued by the APB in the UK, as well as INTOSAI. The NAO Financial Audit Manual supplements and does not replace the SASs. It provides guidance on their application to NAO audits and in addition covers matters which stem from the particular responsibilities of the Comptroller and Auditor General as the statutory auditor of government.

2.5 Professional Bodies

Professional bodies such as the Information Systems Audit and Control Association (ISACA) have established their own standards for the audit of computerised information systems. Whilst these cannot replace international and national auditing standards as detailed above, they supplement them in specific areas of audit and members of these professional bodies must comply with them.
ISACA General Standards for Information Systems Auditing

Certified Information Systems Auditors (CISA) are auditors who satisfy the academic and professional requirements of ISACA. All members of ISACA are required to have a good understanding of ISACA’s General Standards for Information Systems Auditing as well as the supporting Statements on Information Systems Auditing Standards, which provide guidance on implementing the Standards.

The Association’s General Standards for IS Auditing apply specifically to IS audits and consist of ten General Standards covering independence, technical competence, performance of work and reporting:

**Table 1: ISACA General Standards for IS Auditing**

<table>
<thead>
<tr>
<th>No. 1</th>
<th>Attitude and Appearance</th>
<th>In all matters related to auditing, the information systems auditor is to be independent of the audited body in attitude and appearance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 2</td>
<td>Organisational Relationship</td>
<td>The information systems audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.</td>
</tr>
<tr>
<td>No. 3</td>
<td>Code of Professional Ethics</td>
<td>The information systems auditor is to adhere to the <em>Code of Professional Ethics</em> (see below) of the Information Systems Audit and Control Association.</td>
</tr>
<tr>
<td>No. 4</td>
<td>Skills and Knowledge</td>
<td>The information systems auditor is to be technically competent, possessing the skills and knowledge necessary in the performance of the auditor’s work.</td>
</tr>
<tr>
<td>No. 5</td>
<td>Continuing Professional Education</td>
<td>The information systems auditor is to maintain technical competence through appropriate continuing education.</td>
</tr>
<tr>
<td>No. 6</td>
<td>Planning and Supervision</td>
<td>Information systems audits are to be planned and supervised to provide assurance that audit objectives are achieved and compliance with these standards is met.</td>
</tr>
<tr>
<td>No. 7</td>
<td>Evidence Requirement</td>
<td>During the course of the audit, the information systems auditor is to obtain evidence of a nature and sufficiency to support findings and conclusions reported.</td>
</tr>
<tr>
<td>No. 8</td>
<td>Due Professional Care</td>
<td>Due professional care is to be exercised in all aspects of the information systems auditor’s work, including observance of applicable auditing standards.</td>
</tr>
<tr>
<td>No. 9</td>
<td>Reporting of Audit Coverage</td>
<td>In preparing reports, the information systems auditor is to state the objectives of the audit, the period of coverage, and the nature and extent of the audit work performed.</td>
</tr>
<tr>
<td>No. 10</td>
<td>Reporting of Findings and Conclusions</td>
<td>In preparing reports, the information systems auditor is to state findings and conclusions concerning the audit work performed, and any reservations or qualifications that the auditor has with respect to the audit.</td>
</tr>
</tbody>
</table>
**ISACA Statements On Information Systems Auditing Standards**

The Association issues specific interpretations of the general standards. These are referred to as “Statements On Information Systems Auditing Standards”. There are currently nine such statements, as detailed in Table 2 below.

**Table 2: ISACA Statements On IS Auditing Standards**

<table>
<thead>
<tr>
<th></th>
<th><strong>INDEPENDENCE</strong></th>
<th><strong>PERFORMANCE OF WORK</strong></th>
<th><strong>REPORTING</strong></th>
<th><strong>PERFORMANCE OF WORK</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attitude and Appearance, Organisational Relationship</td>
<td>Evidence Requirement</td>
<td>Audit Reports</td>
<td>Use of Audit Software Tools</td>
</tr>
<tr>
<td>2</td>
<td>Involvement in the Systems Development Process</td>
<td>Due Professional Care</td>
<td>Audit Considerations for Irregularities</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>The Use of Risk Assessment in Audit Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Audit Documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The ISACA Code of Professional Ethics**

ISACA Standard No. 3 requires the information systems auditor to adhere to a *Code of Professional Ethics*. This Code of Professional Ethics provides guidance for the professional and personal conduct of members of the Association and holders of the Certified Information Systems Auditor (CISA) designation. It is itemised overleaf.
The ISACA Code of Professional Ethics states that members shall:

- Support the establishment of and compliance with appropriate standards, procedures and controls for Information Systems;
- Comply with Information Systems Auditing Standards as adopted by the Information Systems Audit and Control Association;
- Serve in the interest of their employers, shareholders, clients and the general public in a diligent, loyal and honest manner and shall not knowingly be a party to any illegal or improper activities;
- Maintain the confidentiality of information obtained in the course of their duties. The information shall not be used for personal benefit nor released to inappropriate parties;
- Perform their duties in an independent and objective manner and shall avoid activities which threaten, or may appear to threaten, their independence;
- Maintain competency in the interrelated fields of auditing and information systems through participation in professional development activities;
- Use due care to obtain and document sufficient factual material on which to base conclusions and recommendations;
- Inform the appropriate parties of the results of audit work performed;
- Support the education of management, clients and the general public to enhance their understanding of auditing and information systems; and
- Maintain high standards of conduct and character in both professional and personal activities.

ISACA has recently issued a completely new set of professional standards under the title of Control Objectives for IT (COBIT); the new standards are unusual in that they bring together financial audit, security and value for money control objectives. ISACA members will be expected to use the framework set out by COBIT.
2.6 Other Bodies

There are other organisations that set their own standards for the audit of computerised information systems. Within the United Kingdom, for example, HM Treasury provides guidance for internal audit units with responsibility for appraising information systems operating within central government. This advice is contained in the publication “The Government Information Systems Audit Manual (GISAM)” first issued by HM Treasury in 1993. The advice is divided into seven main sections which deal with:

- Overview;
- Scope and Planning;
- Staffing and Training;
- Approach and Methodology - General;
- Approach and Methodology - Specific Subjects;
- Systems Objectives, Risks and Controls; and
- Potential Audit Procedures.
3. ORGANISING IT AUDIT

3.1 Introduction

Auditing in today’s computerised environment demands that the audit manager possess an ability to assess the level of expertise required to give audit cover to computer based systems, to identify the sources from which staff may need to be recruited, to determine the best method of deploying such expertise within the audit body and to identify the methods of training available for audit staff.

Understanding the developing IT environment is important because:

- The technology and its associated jargon can create problems in communications between IT specialists and auditors. Auditors should be able to close this gap to provide a full and proper audit service;
- General auditors and their managers may feel uncomfortable about undertaking quality assurance reviews of work performed by IT audit specialists.

There is no single solution to these problems and managers need to determine the skills required within their audit team and then work out the most effective way of securing and maintaining that skill base.

3.2 Relevant Skills

All audit staff should have an appreciation of IT irrespective of the amount of day to day contact that they may have with computers and computer based systems.

The need for suitably skilled and competent staff in the audit of computer information systems is embodied in the International Auditing Standard ISA 401:

*Skills and competence*

The auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise and review the work performed. The auditor should consider whether specialised CIS skills are needed in an audit.

Specialised skills are needed to:

- obtain an understanding of the accounting and internal control systems affected by the computer information systems environment and its effect on the business operations of the entity;
- determine the effect of the computer information systems environment on the assessment of overall risk and of risk at the account balance and class of transactions levels;
- design and perform appropriate tests of control and substantive procedures; and
- evaluate the results of the procedures performed.

All auditors, whether generalist or specialist, should therefore be able to participate in the review and appraisal of the adequacy and application of internal controls in computer systems. Specialist staff may also be needed with varying degrees of knowledge and skills to audit the more technical and
complex elements of computer systems. If specialised skills are needed, the auditor should seek the assistance of a professional possessing such skills, who may be either on the audit body’s staff or an outside professional. When using the work of a professional, the auditor should obtain sufficient, appropriate audit evidence that such work will be adequate for the purposes of the audit, in accordance with ISA 620 “Using the Work of an Expert.”

The range of skills needed by staff will be dictated by the nature of auditees’ computer operations, but is likely to include the following:

<table>
<thead>
<tr>
<th>Basic skills and knowledge</th>
<th>Advanced skills and knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>• databases;</td>
<td>• the application and management of various CAATs and generalised audit software;</td>
</tr>
<tr>
<td>• access control software;</td>
<td>• project design and control methodologies;</td>
</tr>
<tr>
<td>• on-line processing (telecommunications and networks);</td>
<td>• systems analysis;</td>
</tr>
<tr>
<td>• operating systems and systems software;</td>
<td>• IT procurement;</td>
</tr>
<tr>
<td>• security, contingency planning and recovery;</td>
<td>• programming languages and generators;</td>
</tr>
<tr>
<td>• micro-computing and office automation;</td>
<td>• IT project management;</td>
</tr>
<tr>
<td>• change and configuration management.</td>
<td>• service level management;</td>
</tr>
</tbody>
</table>

The basic skills and knowledge listed at (1) above are more “control” related, whereas the advanced skills and knowledge listed at (2) include aspects of value for money and security audit as well as controls. By identifying the demands for specific levels of skills, auditors will be able to determine a strategy for addressing any shortfall in IT audit staffing, knowledge and skills; the strategy should have regard to:

- the need for close integration and communication between IT and general auditors;
- the need for a professional focus for the IT audit profession;
- the cost and lead time associated with developing the knowledge and skills of existing staff;
- the availability of, and lead time for recruiting, staff with required IT audit skills; and
• the possibility of short-term appointments of specialist IT staff to provide non-audit technical expertise.

3.3 Acquiring Skills

The initial choice for audit managers is to either:

• use consultants; or
• develop in-house expertise.

It may be more cost-effective to employ consultants to undertake, or advise on, audits of highly technical and complex elements of Information Systems than to develop in-house the necessary skills which may only be used occasionally. Furthermore, smaller audit organisations may experience greater difficulty than larger bodies in obtaining relevant expertise, either through recruitment or training. As a result they may decide to obtain assistance from consultants. The recruitment of external consultants is considered in Section 7.

If the audit office does decide to develop in-house expertise then they need to provide:

• a focus for IT audit research and policy;
• a source of guidance and training;
• a focus for professional development;
• arrangements for consultancy support to deal with complex technical issues;
• policy and procedures for quality assurance review of IT audit products.

3.4 Selection of Specialist Auditors

Computer audit specialists may be recruited directly, or they may be selected from among the general audit staff and given the necessary technical training. However, with the growth in complex systems and the use of techniques such as computer audit programs, there is an increasing opportunity for using technical computer staff as computer audit specialists. A potential recruit’s technical background should be assessed and compared with the current and future IT audit resource/skill requirements. Assessors should be sufficiently qualified to evaluate a potential recruit’s IT technical knowledge, experience and ability.

3.5 Organisation of IT Audit Function

Specialist IT Audit Approach v. Integrated Audit Approach

Auditing bodies need to decide whether to establish a separate group of computer audit specialists, or to opt for an integrated approach where a specialist is part of the general audit team responsible for a group of auditees. Where a specialist team has been established it may only need to be involved in audits involving the more complex computer information systems environments; generalist auditors could carry out work on other audits with specialist advice where necessary. It is, of course, necessary to train the generalist auditors to recognise factors which should lead to a request for specialist advice.
Specialist IT Audit Approach
Advantages of having a specialist group include the reduced time needed to prepare for IT audits and the enhanced credibility it gives to the results and reputation of the auditors. Its main disadvantages are that it requires its own plans, staffing policies, recruitment policy and general co-ordination within the rest of the audit body. Total centralisation can lead to poor integration with general audit.

Integrated Audit Approach
The advantage of an integrated approach is that it sustains an understanding of computer information systems amongst all auditors. Its main disadvantage is that specialist skills may be diluted or lost. Total dispersal can lead to the atrophy of the IT audit function.

Specialist IT Audit Teams - Organisational Requirements
Audit bodies with separate IT audit teams should establish:

- clear arrangements for overall leadership and management to avoid any inconsistency in standards of documentation, evidence and approach;
- an approach which provides an overall evaluation of control (covering duplicated or compensating controls for example) and allows the provision of an overall assurance;
- clear definition of boundaries and interfaces to prevent omission or duplication of work;
- sufficient time for IT auditors to provide specialist advice and assistance; and
- a clear understanding of the respective responsibilities of generalists and specialists.

Specialist units are generally more suited to larger audit organisations while smaller bodies may best opt for the integrated approach with consultancy support as necessary.

3.6 Scheduling Audit Resources
IT auditors are a limited resource in most audit organisations and their time should be appropriately planned and scheduled. Organisational arrangements for IT audit are largely, but not exclusively, governed by the auditing body’s size and its approach to planning. Other factors include:

- the location, variety and complexity of auditees’ computer information systems;
- the availability and cost of appropriately skilled staff;
- the extent of integration of general work with IT audit;
- the level of assurance required by the Audit Manager; and
- any decision to contract out all or part of the audit work.

It is desirable to allocate specific responsibility within an audit body for development, organisation and training in respect of computer auditing. In carrying out the work, at least two levels of skill are necessary - general audit staff and computer audit specialists.
Functions of General Audit Staff in IT Audit
The main functions of general audit staff in this area may be summarised as follows:

- The recording of the preliminary understanding of less complex computer-based accounting systems to determine audit strategy, and the updating of the understanding for all systems after the first year.
- The recording of the system and evaluation of the manual controls in respect of less complex computer-based accounting systems.
- The carrying out of the tests of controls and substantive tests on the annual audit, other than for IT controls and where computer audit specialists make use of computer-assisted audit techniques.

In addition, it is the responsibility of the general audit staff to ensure that the computer audit specialists are called in at the appropriate time to carry out audit strategy and subsequent work, or where there is doubt whether the most current and effective computer audit techniques are in use.

Functions of Computer Audit Specialists
The principal functions of computer audit specialists may be summarised as follows:

- Conducting the preliminary review of complex computer-based accounting systems (or, where major changes have been made to computerised systems, a subsequent review) to gain an understanding of the system and determine audit strategy. This will include making recommendations regarding the potential use of computer audit programs and, where an extended assessment of controls is to be performed, whether the work should be carried out by computer audit specialists or general audit staff.
- The evaluation and testing of IT controls. This work is seldom carried out by general audit staff because of its technical nature.
- The recording of the system and evaluation of manual controls over complex computer-based accounting systems.
- The setting up and running of computer programs in the first year of use. In many cases, for reasons of technical difficulty, computer audit specialists will continue to run them on behalf of general audit staff in subsequent years. Other computer-assisted audit techniques such as test data and program code analysis will usually be carried out by computer audit specialists.

In addition, computer audit specialists would be available to give any other assistance, such as commenting on the content of management letters, or carrying out a security review as requested by general audit staff or the auditee. Work carried out by computer audit specialists should be reviewed and approved by computer audit managers.

3.7 Assessing priorities
Resource limitations, primarily the availability of sufficiently trained and experienced IT auditors, will restrict the number of IT reviews which can be carried out in any given year. Hence, it will not be possible for the IT audit teams to review all computer systems every year.
To enable management to decide where the scarce IT audit resources should be allocated, audit planners will need a method of assessing priorities of work across all auditees. It is likely that generalist auditors will be the main force in influencing the preparation of the IT audit teams’ future workplans, i.e. where generalist auditors have to certify computer generated statutory accounts it is likely that the services of the IT audit specialist will be called upon.

Where an IT audit team can decide upon its forward workplan of IT reviews, there are several factors which should be considered. These are outlined below.

Materiality
The value of the computer systems themselves, the value of the transactions they process, and the value of the business programmes they support.

Security
Systems which process sensitive transactions or hold confidential data, e.g. personnel systems and defence computers, may derive benefit from an IT review. Security considerations will include confidentiality, integrity and availability.

Degree of user involvement
Systems which have been developed with little user involvement are less likely to meet user requirements. User involvement may include the needs of external auditors (e.g. audit trail, document retention etc.).

High development costs
Systems with high development costs are likely to be more complex and have more ways of failing. High development costs may indicate that a system has been poorly designed and may fail to meet user requirements.

Technological complexity
Technologically complex systems may be subject to new audit risks. Generalist auditors are unlikely to have sufficient IT experience to review these systems. The increasing complexity and interconnection of IT systems is likely to increase the demand for specialist IT audit support.

Specific request for system review
Requests can be received from a number of sources, including political groups, the media, pressure groups or the auditee itself.

Parliamentary interest
Parliament may be interested in a particular IT system and may expect that a review will be carried out. Parliamentary interest can change the auditors’ assessment of what is a material system.

Increased Parliamentary interest in IT system failures, IT fraud and abuse is likely to target generalist audit interest in information systems and hence more request for specialist support and advice.

Contribution to profit or to operational control
Systems which are essential to the continuing operation of an auditee’s business.

Impact on customers or customer services
Systems which have a high impact on customers, for example a social benefit payment system.

**Contribution to decision making**

Systems which may affect the processing and/or decision making processes of other systems. Where the output from one system may form the input to several others.

**History of poor performance/problems**

Where systems have gone wrong in the past, there is a real risk that lessons will not have been learned and the same or similar problems re-appear.

**Depth/ scope of internal audit coverage**

The external auditor may be able to place reliance on the work of an auditee’s internal audit function. Before any reliance can be placed, the auditor must gain assurance that the work of internal audit is satisfactory.

**Changes in audit approach**

Changes in audit approach may lead to increased reliance on systems controls and hence increased emphasis on reviews of auditees’ IT systems.

**Effects of outsourcing of IT functions**

The outsourcing of IT functions and the need to exercise inspection and access rights will affect the demand for IT audit services.

**Development of a Strategy to Meet the Demand for IT Audit.**

Possible measures to improve the **quantity** of support available include:

- secondments to the IT audit teams from line units;
- use of contractors/ consultants; and
- IT trained auditors on line units.

Possible measures to improve the **quality** of IT audit resources include:

- professionalism (e. g. CISA);
- continuing education and development of IT auditors;
- secondments of IT auditors to external consultants/ contractors;
- IT and IT audit training for generalist auditors; and
- the development of a framework for improved co-ordination of IT auditors with generalist auditors.

**Balancing Total Resource Requirements to Available Staff Resources.**

Where resources are less than the workload, the audit manager should consider:

- buying-in resources;
- cancelling or re-scheduling work; or
• outsourcing work.
Where resources are greater than workload, the audit manager should consider:
• more ad hoc reviews;
• secondments to consultants;
• increased developmental work; or
• mainstream financial audit/value for money audit.

Common Problems when Planning
Demand-led IT audit work
Generalist auditors call upon central resources to assist them with their audits when they feel that they need expert help. Line auditors may not know that they need help until they begin their audit and experience difficulties when confronted by an IT system. When they call for assistance they usually expect it to be readily available. Hence IT auditors may not know and be required to estimate or guess how much assistance they will be required to give, when it will be required or how complex each particular job will be. It is difficult to plan when you do not know what you are planning for.

Ad hoc work required to be undertaken urgently
As central resources and the “IT experts”, those involved in IT audit will invariably be required to carry out almost any IT related activity, for example:
• dealing with senior management queries;
• contribute to responding to public letters;
• training line auditors on IT audit issues;
• attending seminars;
• international liaison (INTOSAI); and
• IT audit development work.

Matching staff skills and experience to each job
Staff with few IT skills should only undertake low complexity IT audits. Managers of IT groups will need to record details of each IT auditor’s skills, training and experience.

Seasonal variations in the workload
Peaks in workload may arise where auditees have a common year end reporting date. For example, in the UK, audit planning for the majority of accounts with a 31 March year end date takes place in the previous October and November. IT auditors should be aware of when the peaks and troughs occur.
Planning for indirect time such as staff sickness (unknown quantity), holidays (annual leave and public holidays) and staff training.
3.8 Planning

It is usual for audit organisations to plan their activities on three levels. Each level of planning is based on a different time frame. These are given below.

**Long-term Strategic Planning**

The timespan of long-term strategic planning is measured in years (usually the next 3-5 years). These long-term plans cover organisations as a whole and usually include sections on individual departments, divisions, units or responsibilities.

- They operate at a high level and set broad objectives for each major type of activity.
- The plans may be reviewed and updated annually.
- The targets and objectives are determined and approved by senior management.

Issues relating to IT audit which may be included:

- where IT audit is going, its aims and long term objectives;
- how the IT audit function will adapt to meet changes, developments;
- resources required for IT audit (staff numbers, accommodation, equipment, financing); and
- training requirements.

**Medium-term Strategic Planning**

The medium term strategic plan translates the long term strategic plan into a programme of work for the coming year. Planning at this level is often based upon a combination of the demands and requirements of the line auditors and central developmental work.

These plans define the aims and objectives of each major audit. They should be sufficiently flexible to cope with changes. Drafting of these plans is normally carried out by middle management. The plans are approved by senior management.

**Operational Planning**

Operational audit plans are based on individual audits and contain details of exactly what is required, when, and how to carry out the audit.

- Operational plans also include details of resource requirements and audit procedures;
- Operational plans are drawn up by the lower management, perhaps with the support of an IT specialist, and approved by middle management.

The IT auditor will usually be tasked with carrying out a review before the generalist auditor prepares his/her detailed operational plan. Once tasked, the IT auditor should prepare an IT audit plan.

**IT Auditor Involvement in the Audit Lifecycle**

The audit process can be split into several lifecycle stages, all of which are applicable to both financial and value for money audit. IT audit specialists can be involved in the majority of the stages.

1. Plan the audit
The IT auditor may be asked to review and document an auditee’s financial IT systems. He/she may also be required to identify developing and material computer systems.

2. Preliminary study or pilot value for money review
The IT auditor may be required to assist with collecting preliminary study evidence, drawing up questionnaires etc.

3. Collect evidence
The IT auditor may be asked to obtain data using CAATs. He/she may be asked to interview auditee staff.

4. Analyse evidence
The IT auditor can use CAATs to analyse data.

5. Draw conclusions / certify the financial statements
The IT auditor’s knowledge of IT best practice may be called upon to draw comparisons of performance or interpret CAATs data.

6. Draft report / management letter
The IT auditor can contribute his/her findings to management letters and reports.

7. Clearance of draft
The IT auditor may be required to clear the more technical audit comments at clearance meetings.

8. Finalise report or management letter and publish/send
The IT auditor may be required to assist in the redrafting of elements of the management letter or value for money audit report.
From the IT auditor’s point of view, the following stages are more likely to be apparent.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 1</td>
<td>The generalist auditor is tasked with carrying out the audit of an auditee’s financial statements or a review of the performance of a business activity.</td>
</tr>
<tr>
<td>Stage 2</td>
<td>The generalist auditor assesses the scope of the audit and identifies whether there are IT systems involved.</td>
</tr>
<tr>
<td>Stage 3</td>
<td>The generalist auditor, or IT auditor if requested at this stage, carries out a general review of the auditee’s IT systems.</td>
</tr>
<tr>
<td>Stage 4</td>
<td>The generalist auditor decides on whether there is any need for specialist IT audit assistance. (His/her decision may be based on advice provided by the IT audit specialist).</td>
</tr>
<tr>
<td>Stage 5</td>
<td>The generalist auditor contacts the IT auditor and they agree the details of the IT review.</td>
</tr>
<tr>
<td>Stage 6</td>
<td>The IT auditor prepares an IT audit plan.</td>
</tr>
<tr>
<td>Stage 7</td>
<td>The IT auditor contacts the auditee, arranges to obtain evidence and then collects it.</td>
</tr>
<tr>
<td>Stage 8</td>
<td>The IT auditor assesses and analyses the audit evidence and draws conclusions.</td>
</tr>
<tr>
<td>Stage 9</td>
<td>The IT auditor provides a report for the generalist auditor.</td>
</tr>
<tr>
<td>Stage 10</td>
<td>The IT auditor and generalist auditor discuss the report and then clear it with the auditee.</td>
</tr>
</tbody>
</table>
4. TRAINING AND AWARENESS

4.1 Training Strategy

Computing is a continuously developing technology. Effective staff training is necessary if an audit body is to acquire and maintain the skills necessary for IT audit. The extent and variety of computer information systems in most auditees means that the auditor needs knowledge and skills across a wide range of subjects. In larger audit bodies it may be possible for an individual to specialise to a greater degree than in smaller bodies. Considerable initial and on-going investment in training should be planned to develop new skills and to update existing skills.

Different training strategies will be needed for different levels of skills - general and specialist. Training should be related to the identified needs of the audit body and should be regularly updated. Training should not be driven by the personal preferences of the individual.

Training can be provided either as part of an overall training programme where manual and computer audit training are integrated, or by separate computer audit courses. In general, the first approach is preferable. Since general audit staff can expect to find computerised systems at the majority of their auditees, it is desirable that all auditing courses which they attend should take account of this fact by dealing with the techniques and methods applied in auditing computerised systems.

4.2 IT Audit Training

Additional IT audit training needs fall into 5 main categories:

- general training in such areas as data automation, hardware architecture and on- and off-line storage facilities;
- specific technical training in operating systems (e.g. VME, AS400), IT methodologies (e.g. PRINCE and CRAMM), IT security and IT project management;
- training directed at enhancing IT audit skills, such as the use of file interrogation software;
- training in legislation governing the use of Computerised Information Systems; and
- training directed at enhancing understanding of the way in which information systems can contribute to auditees’ effectiveness and efficiency; this may include further training about Management Accounts and Executive Information Systems.

A variety of sources and training methods exist to address technical training needs. Sources include the same courses as those attended by the auditees, manufacturers’ courses, use of in-house facilities, training provided by other IT training institutions and computer-assisted learning packages. These last have the advantage of being available at the work place and learning takes place in line with individuals’ capabilities.

Feedback on training should be obtained from students immediately after training and again in 6 months to evaluate the effectiveness of the method chosen.
4.3 Qualifications

Specialist qualifications that may be relevant are the ISACA Certified Information Systems Auditor (CISA) qualification, or a qualification issued by a national professional body (such as the British Computer Society Examination, and the IIA-UK Qualification in Computer Auditing). These complement staff training by providing certificated evidence that an auditor has practical and proven experience in the appraisal of computerised systems.

4.4 Training Logs

Details of all training undertaken, qualifications achieved and experience gained should be recorded in each auditor’s personal log book and reviewed from time to time. This will allow both the auditor and the auditing body as employer to ensure that the auditor’s training needs are being met and directed. It will also serve the purpose of complying with the requirements of professional bodies to demonstrate an acceptable level of continuing professional education is being achieved.

4.5 Technical Library

Each IT audit office should establish and maintain a technical library that will provide staff with up-to-date guidance in the performance of IT audit, as well as keep them abreast of the latest views on issues to affect them, such as the development of standards. It is helpful to keep in one place copies of audit letters and reports commenting on weaknesses in IT controls. In this way computer audit specialists can read of recent experience. A further function of such a library is to keep staff informed of developments in the IT industry, by bringing to their attention the latest innovations in technology. A technical library could include the following:

- Auditing standards;
- Statutory legislation;
- Professional institutes’ standards and guidance;
- Auditee manuals;
- Text books;
- Prior years’ IT audit reports;
- Professional journal subscriptions;
- Trade magazine subscriptions;
- University faculty reports and newsletters;
- Training course manuals;
- Consultants’ reviews/dissertations/reports;
- Hardware and software suppliers’ manuals, brochures and sales material;
- Press cuttings.
4.6 Development Work

If a computer audit group is established, it should normally be responsible for developing the audit body’s computer audit techniques and approach under the direction of the relevant committee or director. The amount of this work will depend mainly on the extent to which it is decided to develop documentation specific to the audit body as opposed to using published material. Larger organisations may choose to design their own documentation so as to integrate this with their existing audit approach and methods. This is likely to apply in particular to the detailed methods of recording the system and evaluating the controls. Considerable technical support is required to develop computer audit software packages to interrogate auditees’ data files and only the larger organisations are likely to find it worthwhile to allocate resources to projects of this nature. Most bodies are, however, likely to find that effective use can be made of standard interrogation, spreadsheet, database or other software packages on microcomputers for such purposes as file interrogation or audit planning. Particular applications of such software may be developed by the computer audit specialists for use by general audit staff.
5. CONTINUING PROFESSIONAL EDUCATION

5.1 Professional Qualifications

Information systems technology is constantly changing. Training and ongoing education should maintain the individual IT auditor’s competency through updates of existing skills as well as training directed towards new audit techniques and technological areas.

Professional bodies such as the ISACA require their members to undertake continuing professional education to maintain their qualification.

ISACA General Standard No. 5 (Continuing Professional Education) states:

“\textit{The information systems auditor is to maintain technical competence through appropriate continuing education.}”

Continuing professional education therefore is not just a desirable, but an essential requirement for IT auditors.

5.2 Workshops, seminars and other forms of CPE

As well as formal training aimed at acquiring or maintaining a professional qualification such as CISA, other less structured means of undertaking CPE should help the IT auditor keep up-to-date with IT and IT audit. The auditor should be encouraged to attend workshops and seminars on a regular basis, as well as study text books, manuals and journals as detailed at paragraph 4.5 above.

Further sources of information on recent developments in the industry, as well as debate, are Internet news groups and bulletin boards.
6. MONITORING AUDITEE DEVELOPMENTS

6.1 Understanding an auditee, Operations and IT Organisation

In order to properly plan and carry out an IT audit, the auditor should have or acquire a sufficient understanding of the auditee’s business and information systems environment to enable him or her to design an audit approach which:

- **is effective** - The auditor obtains sufficient appropriate evidence to support their opinion;
- **is efficient** - The auditor targets resources on the areas of greatest risk and chooses methods which meet objectives at minimum cost;
- **adds value** - The auditor offers auditees constructive advice on IT management and control relevant to their circumstances.

The auditor’s understanding will include an identification of the organisation’s reporting framework, business objectives and practices, legal and regulatory environment, as well as information on the IT system used. This understanding will inform the risk assessment, as well as identify such practical matters as the staff to deal with, geographical locations and so on.

It goes without saying that the auditor should ensure that this understanding is based on up-to-date information gathered from a continual review of auditee developments. Standing data from the prior year’s audit is a starting point, however this should be carefully reviewed to ensure that it is still relevant. All changes in the auditee’s business and IT environment should be monitored and their impact on the audit assessed.

- Matters usually considered include:
  - the entity’s use of and attitude towards information technology and the effect of this on the nature and source of systems applications - for example, the extent to which the entity purchases recognised and proven systems applications or develops systems applications in-house or under contract;
  - use of information technology by the entity compared with general usage within the industry and the local environment within which the entity operates, as well as information technology trends - including generally available information about computer information systems usage by competitors and trading partners; and
  - recent and planned changes to the entity’s information technology and information technology environment - for example, outsourcing the information technology department, changing the technical platform and changing leadership and business direction.
6.2 Sources of Information

The IT auditor can usually obtain this information from:

- the general review of IT;
- internal audit reports;
- past audit experience or history;
- discussion with management, IT and internal audit personnel;
- monitoring and marking (annual reports, industry publications, independent analyst reports and regulator reports);
- annual budgets / resource bids (estimates);
- IT strategy documents;
- post-implementation reviews;
- policy statements (government, auditee);
- the auditee’s business plan;
- Board minutes;
- the minutes of key IT committees;
- site visits; and
- press cuttings.

Having an understanding of the auditee’s business will enable the IT auditor to determine what the most likely risks are. This knowledge will ensure that resources are focused on these risk areas.

6.3 General Review of IT

A preliminary survey is normally carried out by the generalist auditor (i.e. a non-IT specialist) in charge of planning the financial or value for money audit, to gather and document information on the auditee’s IT systems. There may be occasions when the generalist auditor will require assistance from an IT auditor in completing the survey, for example where auditees have large computer departments with several complex IT systems.

The survey should be completed as part of preliminary planning. The intention is that, once completed, it could be handed to whoever will be carrying out the full scale review of the IT systems (either the IT specialist or generalist auditor depending on the situation).

A completed survey should be sufficient to enable the IT auditor to understand what he/she is dealing with in terms of the auditee’s hardware and software, IT personnel and the nature and extent of any known problem areas. The survey is basically an introduction to the auditee’s IT.
6.4 IT Legislation and Regulation

Furthermore, each auditee organisation, regardless of its size or the industry within which it operates, will need to comply with a number of government and external requirements related to computer system practices and controls and to the manner in which computers, programs and data are used. Special attention should be given by auditors to these issues in those industries, such as financial services, which are regulated closely.

The IT auditor must:

- Identify those government or other external regulations or requirements that deal with computer system practices and controls; the manner in which computers, programs and data are stored; and that are relevant to the organisation or to the activities of the IT function.
- Document pertinent laws, regulations etc.
- Assess whether the management of the organisation and the IT function has considered the relevant external requirements in making plans and in setting policies, standards and procedures.
- Review internal IT function documents that address adherence to laws applicable to the industry.
- Determine adherence to established procedures that address these requirements.

6.5 Documentation

It is essential that auditors document, maintain and update their knowledge of the auditee’s business and information systems environment, keeping abreast of any changes to existing computer information systems; the introduction or development of new systems; changes to legislation; changes to reports and other outputs; changes to business objectives; changes to personnel and so on. This will involve a formal monitoring of auditee developments, which should be documented in permanent files in order to provide future audit teams with a comprehensive and up-to-date picture of the background to the IT audit. It should not be assumed that changes will only affect the auditee and not the audit team.

Corporate standards for the documentation of auditees’ information systems and controls will assist in the handover process when there are changes in the audit team.
7. EXTERNAL CONSULTANTS

7.1 Introduction

It may be more cost-effective to employ consultants to undertake, or advise on, audits of highly technical and complex elements of Information Systems than to develop in-house the necessary skills which may only be used occasionally.

It may also be cost-effective to:

- market test the entire IT audit service;
- employ consultants to support and develop the unit’s IT audit strategy and approach;

Consultants may also be used for specific audit tasks where the necessary skills are not available in the audit body. Skills transfer should be an important objective of such arrangements.

It is important to control the cost of using consultants. The working relationship between auditors and consultants should demonstrate value for money. Contractual arrangements should be established in a manner which allows the audit body to maintain an IT audit approach conforming to appropriate audit standards.

To get the best results from the use of consultants, it is important to:

- identify tasks, opportunities and new approaches where their experience and expertise could benefit the audit;
- select the right consultants for the job (there are a lot of “cowboys” about - look for a proven track record by taking up references);
- bring them in early;
- set firm objectives, clear terms of reference and tight budgets;
- integrate the consultants’ contribution with the work of the rest of the team;
- supervise and manage the work through to a successful conclusion; and
- learn lessons for the future.

The following guidance on the selection and use of consultants should help provide a close working relationship that will ensure a successful partnership.

7.2 Why Use Consultants?

The possibility of using consultants, and on what tasks, needs to be considered in the early stages of planning the work. Deciding to bring in consultants after an audit has started is unlikely to be successful. It can take up to three months, and sometimes longer, from identifying the need to issuing the contract.

Always try to alert consultants to possible requirements for their services in good time, both on specific tasks and more generally. They can then plan ahead to help ensure that they are in a position to offer assistance. Too short a period of notice makes it difficult for them to respond to best effect,
and to put forward the right staff. Their most appropriate staff resources may be booked up months in advance.

The main reasons for using consultants are:

- to tap into outside experience and expertise and draw on wider disciplines and specialist skills;
- to add breadth and penetration to examinations;
- to identify new approaches and introduce different perspectives;
- to survey best practice in relevant outside fields and activities;
- to provide a cross-check on the auditor’s own approach, method and costs;
- to provide extra resources to meet peak workloads;
- to advance delivery dates and help to meet deadlines; and
- to add weight to findings, conclusions and recommendations.

### 7.3 What Kind of Consultant?

There are no fixed rules on what kind of consultants are best suited to particular tasks or projects. Costs as well as benefits need to be compared in deciding which type of consultancy to choose. The consultant chosen will need to have the resources and ability to meet tight deadlines and possible changes as the work develops.

In practice, the choice is likely to lie within one of three broad categories:

- a consultancy firm or similar organisation;
- an individual or group with an academic or research involvement in the subject or area under examination, or skilled in relevant disciplines or analytical techniques; and
- someone with in-depth experience and an expert practical background in relevant operations or business activities.

**Consultancy firms** command the largest resources and are able to offer a wider range of services. They have the advantage of being able to draw on a variety of disciplines to provide teams of staff and managers to work in the field as part of the main investigation. It is important to remember that the necessary expertise may be found in the smaller specialist firms as well as the larger management consultancy groups.

**Individuals** might typically be used to advise on strategic planning and preparatory work as well as on specific examinations. They can be used as part of an audit team, but it is often much easier to use them flexibly - in short concentrated bursts - at successive stages of an examination. Working in this way can be highly cost-effective as well as being attractive to the individuals concerned, since their time is not then tied up for long periods. People who have recently retired from the audited body, or other relevant organisation, should also be considered. They may already be well versed in the audit or operational background to the work.

Both consultancy firms and individuals may be used to review strategic thinking and to suggest ideas for future directions or areas of work. They may advise on plans for individual examinations, and be
brought back to review emerging fieldwork results and provide further analysis. They may be used to review final results and the conclusions and recommendations to be included in reports. Their contribution and support are often valuable in the final clearance discussions with auditees.

7.4 Notifying the Auditee

The intention to use consultants on audit examinations should be discussed with the audited body at an early stage. They should also be kept informed as necessary as the work progresses and results emerge.

Although the audited body’s views should be fully taken into account, decisions on selection and use of consultants are ultimately the responsibility of the auditor.

Good communications with the audited body gives them the opportunity to:

- put forward any general reservations or suggestions about using consultants;
- confirm their acceptance that the prospective consultants can, in principle, be expected to produce soundly based and authoritative conclusions;
- raise any questions about the access the consultants will need to auditee records, documents and other information, including compliance with Official Secrets Acts or other requirements;
- discuss potential difficulties over individual consultants or consultancy firms, for example on security grounds, on commercial confidentiality or because of possible conflicts of interest with other work; and
- seek information on how the results of the consultants’ work will be handled during and at the end of the examination.

7.5 Short-listing Candidates

Having decided on the type of consultancy required, the next step is to identify possible candidates.

Once possible consultants have been identified, further informal enquiries - for example by telephone - should enable a short-list to be drawn up of those available to undertake the assignment and interested in quoting for the work.

These initial discussions are valuable in providing an opportunity for an early assessment of the capabilities of potential bidders. Avoid building up a special or preferential relationship with any individual or consultancy firm competing for the work or otherwise giving them an advantage in securing the assignment. Competitive tenders should be the normal rule.

Make an initial selection from such sources as:

- consultants who have previously carried out successful assignments;
- enquiries amongst known experts in the field;
- professional bodies and similar organisations;
- standard reference sources, for example directories; and
- suggestions by the audited body.
7.6 Financial Control

Likely costs have to be considered at all stages of the work. It is the project manager’s job to ensure that sufficient funds are available for the assignment; that costs and commitments are monitored against approved budgets; and that costs are contained and penalties avoided.

However, it is important to remember that costs aren’t everything. The quality, speed and timeliness of the work are also crucial factors. Keeping costs under tight control is essential, but it would be foolish to jeopardise the usefulness of the work, and perhaps hinder the investigation as a whole, by taking concern for costs too far.

To ensure sound financial control:

- draw up a specification of the objectives, scope and timing of the assignment;
- prepare a provisional estimate of fees and expenses as soon as possible, and certainly before going out to tender;
- confirm availability of funds and provisional budget approval;
- review the scope of the work and/or budget in light of tenders submitted and confirm revised approval as necessary;
- monitor costs against budget as work proceeds and agree prices in advance for any extra work to be carried out; and
- revise work plans to keep within approved budget, or obtain revised approval as necessary for essential extras.

7.7 Seeking Bids

Bids should normally be obtained by competitive tender. Single tender action may be appropriate where the assignment extends an existing contract won in competition, or where there is clearly only one source of assistance. Exceptionally, this may also be necessary where time is very short. Each auditing body should have established tendering procedures, set out in writing. Consult the appropriate authority for these tendering requirements.


## 7.8 Assessing Proposals

It is important to decide in advance the criteria to be used to evaluate the individual proposals received from consultants. The main questions to be asked when assessing individual proposals are set out below.

<table>
<thead>
<tr>
<th>Assessing Consultants’ Proposals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are the consultants experienced in the field under examination? Are they well versed in public sector concepts?</td>
</tr>
<tr>
<td>Can they demonstrate achievements and results in relevant areas? Have they a good track record?</td>
</tr>
<tr>
<td>Do their proposals conform to the terms of reference? Do they demonstrate a sound grasp of the aims and objectives of the assignment?</td>
</tr>
<tr>
<td>Have they analysed the task requirements carefully and thoroughly? Are their approach and methodology sound?</td>
</tr>
<tr>
<td>Are the individuals who will personally undertake the work capable, experienced and of high quality?</td>
</tr>
<tr>
<td>Is there a clear commitment of partner and senior management back-up?</td>
</tr>
<tr>
<td>Will additional resources be available as necessary to help overcome any problems?</td>
</tr>
<tr>
<td>Are they committed to the timing of the work and meeting the agreed deadlines and delivery dates?</td>
</tr>
<tr>
<td>Do they recognise the importance of clear control and reporting arrangements?</td>
</tr>
<tr>
<td>Are the costs firm and clearly set out? Does the bid provide an appropriate analysis of time and charge-out rates? Are expenses and other costs clearly identified? Are there any “hidden extras”?</td>
</tr>
</tbody>
</table>

## 7.9 Working Relationships

Good working relationships are essential to get the best out of consultancies. All aspects of an examination should remain under the auditor’s control, but it is important to remember that the consultants are an important part of the team and will provide better value for money by being given every opportunity to deploy their experience and abilities.

- Make sure the consultants are kept fully briefed on the objectives of the work as they develop.
- Provide them with the information and co-operation they need to do the job. Keep them up to date with the work of the rest of the team and involve them as necessary in team discussions.
- Brief the consultants on any expected or emerging problems - for example on access to information or sensitivities in relationships - and procedures for resolving them.
- Explain normal arrangements for dealing with the auditee and ensure that the consultants follow them.
- Make it clear that important discussions on findings with the auditee will be led by the auditor. The consultants will, of course, be expected to play a full part in such discussions but should never take over the lead role.
• Watch for any risk of confrontation between specialist consultants and the auditee’s own experts.
• Make it clear that the consultants’ role as part of the team means that they will operate under the overall management of the team leader.

7.10 Managing the Work

The project manager should make sure that the consultants provide the results expected. This means identifying the crucial elements in the assignment, keeping the consultants informed and monitoring and controlling the various stages of the work. Keeping control of contractors means ensuring that the contract specifies frequent, measurable deliverables and then tracking progress against the agreed schedule. Firm oversight and prompt action are needed.

Working effectively with the consultants means the project manager should:
• set up the necessary liaison arrangements, including timing of interim reports and meetings at key stages;
• make sure from the outset that there is a clear understanding about the scope of the consultants’ work, timetable and deadlines;
• encourage two-way traffic and an effective working relationship between the consultants and the rest of the team;
• establish arrangements for identifying and dealing with any emerging problems;
• ensure that any variations to the work, and extra costs, are cleared and approved in advance and the contract amended accordingly; and
• review and discuss the consultants’ reports promptly, linking their findings with the work of the rest of the team and ensuring feedback.

7.11 Reviewing Findings

Work done by consultants in effect becomes the work of the auditor. It is not possible to hide behind their reputation or expertise. Therefore, their findings and conclusions need to be independently reviewed to ensure that they meet the required standards.

In specialist fields this may not always be easy, but it cannot be avoided if the final report is to be presented to the auditee and to addressees such as Parliament on a defensible basis.

When reviewing the consultants’ work the auditor must:
• be satisfied that the coverage has been carefully planned and that the fieldwork has been properly carried out and is based on sound, documented evidence;
• ensure that the findings and conclusions in the consultants’ report are accurate, fair and balanced;
• watch that recommendations are practical and cost-effective;
• check the consistency of their work, findings and recommendations with those of the rest of the audit team;
• pay special attention to those aspects which have caused, or are likely to cause, particular difficulties with the audited body; and

• discuss and resolve potential difficulties with the consultants, and seek their advice on how their work can best be used.

**7.12 Consultants’ Reports**

Careful consideration needs to be given to the best ways of dealing with the consultants’ findings when deciding on the content and presentation of the final report to be published. Whichever course is adopted, it should be made quite clear that the audit body stands by the end product and does not distance itself from the consultants’ findings.

In some cases, consultants may wish the results of some or all of their work to be published separately, or used for other purposes. This requires the auditing body’s approval and cases should be considered on their merits in consultation with the auditee.

Consultants’ findings may be used in the following ways:

• no written report by consultants, but findings discussed and incorporated as necessary in final published report;

• consultants submit written report to the auditor, but this is wholly subsumed within the final report;

• consultants’ findings are included in whole or in part in final report, and are identified accordingly;

• consultants’ report, or summary, is included as a separate chapter or annex in the final report; and

• consultants’ report is published separately by the audit body, as complimentary to the main report.

**7.13 Assessing Performance and Learning Lessons**

It is important to realise the full benefits of the consultancy by learning lessons for the future. This also helps to build up a record of performance as a basis for placing future work. Reviewing the work should be done in frank discussion with the consultant and with the rest of the audit team. The aim should be to learn lessons from successes achieved as well as from any difficulties encountered.

Reviewing the work should be done as quickly as possible, whilst thoughts on both sides are fresh, and a brief written report produced, highlighting good and bad points and assessing the consultants’ overall performance.

Main aspects to be covered include:

• Whether the work met the agreed task objectives?

• Whether it was completed within the approved programme and timescale?

• Whether it was delivered within the agreed cost?

• What difficulties arose and why?
• Whether problems were anticipated, or spotted at an early stage, and satisfactorily resolved?
• Whether there was good co-operation and co-ordination with the rest of the audit team?
• Whether the results of the consultants’ work were soundly based? Did they make a valuable contribution to the final report?
• Whether the consultants provided other “added value” to the examination?
• What ideas and suggestions do the consultants have for improving future arrangements?
• Whether there are any other lessons for the future?
8. IT AUDIT APPROACHES

8.1 Why and When to Use an IT Auditor

Types of Audit

The fundamental scope of an IT audit is no different to that of an audit carried out for the same purposes in a non-computerised environment. However, the objectives or scope of the audit will differ with the type of audit being carried out. Different types of audit are:

- Financial Audit;
- Value for money Audit;
- Security Audit;
- Forensic Audit.

Financial Audit

In financial audit the auditor aims to test the integrity of the assertions made by management in the financial statements regarding:

- Existence;
- Rights and Obligations (Ownership);
- Occurrence;
- Completeness;
- Valuation;
- Measurement;
- Presentation and Disclosure; and
- Regularity (in the central government sector).

The auditor therefore confines his or her work to financial systems.

Value for money Audit

In value for money audit the auditor aims to test systems as to:

- Economy;
- Efficiency; and
- Effectiveness.

The work of the auditor is not confined to financial systems.

Security Audit

In security audit the auditor aims to test all systems as to their:

- Confidentiality;
• Integrity; and
• Availability.

The auditor’s objective is to assess whether management have undertaken sufficient work to reduce residual risk to an acceptable level.

**Forensic Audit**

In forensic audit the auditor’s work is investigative. Through the analysis of systems and stored information, he or she seeks to explain irregularities, anomalies or fraud.

**Internal vs. External Auditors**

Auditors may be categorised as:

• Internal Auditors; or
• External Auditors.

The distinction between the two can be defined by the particular audience to which each presents their audit opinion.

**Internal Auditor**

The work of an internal auditor is defined by INTOSAI as follows:

“*The functional means by which the managers of an entity receive an assurance from internal sources that the processes for which they are accountable are operating in a manner which will minimise the probability of the occurrence of fraud, error or inefficient and uneconomic practices. It has many of the characteristics of external audit but may properly carry out the directions of the level of management to which it reports.*”

Internal auditors therefore report to the management of an entity and are often involved in system development and management services. They look at all internal controls - not just financial controls.

**External Auditor**

The work of an external auditor is aimed at providing an independent opinion as to the probity of financial statements for the benefit of the owners (shareholders, parliament, Board and so on) of an entity and NOT on the behalf of management.

**IT Audit vs. Non-IT Audit**

If the fundamental scope of an IT audit is no different to that of an audit carried out for the same purposes in a non-computerised environment, why then should IT audit be treated differently from non-IT audit? Why do we have IT audit specialists who use their own audit methods and tools?

The answers to these questions lie in the fact that IT systems have different characteristics and associated risks which require the auditor to have additional skills and experience.

For example, IT systems may:

• allow anonymity and reduce accountability;
• permit unauthorised and unrecorded amendments to be made to accounting data;
IT auditors are a reasonably scarce resource. Their skills and experience will not be required for all IT reviews. The general auditor has to make a judgement about the need for IT audit support. This decision should be based on factors such as those given in the table below.

**Factors to consider when deciding to call in an IT auditor:**

- the size of the auditee’s IT systems;
- the sophistication and complexity of the auditee’s IT systems - e.g. distributed systems;
- the nature and extent of risks associated with the use of IT - e.g. new technologies such as EDI;
- where the auditee demands or expects the use of an IT audit specialist;
- where there have been previous problems with staff in the IT department;
- the scale of in-house IT developments;
- where there have been significant changes to important systems;
- where computer systems are vital to the auditee’s business;
- where stakeholder (public, media, parliament) pressure requires an IT specialist;
- where there is a history of computer errors, fraud or IT security breaches;
- where there is evidence of poor IT performance;
- where complex CAATs may be used.

**The generalist auditor may not need a specialist IT auditor if:**

- the auditee has a simple IT system;
- the auditee has commonly used computer systems with few, if any, modifications or bespoke elements;
- there have been few or negligible changes to the system since the last IT review.
8.2 INTOSAI IT Audit Curriculum

Once the generalist auditor has decided to call upon the services of an IT auditor, the IT audit section’s management will then have to decide on what level of IT audit skills are required to carry out the review, and hence which IT auditor should get the job. The INTOSAI IT audit curriculum can assist management in making this decision.

The curriculum is based on the assumption that there are three levels of IT audit skills:

**Level 1: the generalist auditor**

This equates to the ordinary auditor, who is familiar with the issues and methods of IT audit, can undertake simple IT audit tasks and can use IT specialists to serve the general audit objectives.

**Level 2: the IT auditor**

The IT auditor is someone who has chosen to specialise in IT audit. These people have sufficient skills and experience to undertake most IT audits.

**Level 3: The expert IT auditor**

The expert IT auditor is someone who, through depth of experience, has become very familiar with IT and IT audit issues, and can undertake or supervise audit tasks including highly specialised ones.

The IT audit curriculum splits IT audit tasks into seven discrete areas and provides guidance, in the form of schedules, on what level of expertise would be required to satisfactorily carry out each. The seven categories of task are shown below. IT audit managers will be required to ensure that suitably qualified and experienced IT audit staff are tasked with carrying out each IT audit review.

**IT Audit Tasks**

- planning an IT audit;
- assessing controls in IT systems;
- computer assisted audit techniques, including microcomputer tools;
- auditing IT systems under development or procurement;
- undertaking value for money audits of IT systems and functions;
- special assignments; and
- reviewing and reporting the results of an IT audit.

8.3 Identification of Material Risk Areas

The auditor’s assessment of risk will affect the timing of the audit and the resources (numbers, skills and experience) needed to carry out the work. The auditor should determine the nature and extent of audit risk, which will be different for each of the following types of audit:

- Financial audit;
- Value for money audit / reviews;
- Developing systems.
Audit Risk in Financial Audit

This can be defined as the risk that the financial statements may contain material error. In financial audit the concept of materiality can be subdivided into materiality by value, nature and context. Determining materiality for each sub-category will depend upon the sensitivity of financial statements. The controls within computerised financial information systems can contribute to the level of assurance the auditor takes by reducing the risk of a material misstatement.

The IT auditor will usually be required to identify computer controls which contribute to reducing audit risk. This will involve identifying controls which reduce:

Inherent risk
The risk of a material error arising in the first place. The IT auditor can assess factors such as the business environment.

Control risk
The risk that internal controls will fail to detect or prevent material error. The IT auditor can evaluate the computer controls.

Detect risk
The risk that a material error will not be detected by audit procedures. The IT auditor can use CAATs to detect material misstatements.

The IT auditor should establish what controls review tools will be used to identify and assess these controls.

Audit Risk in Value for money Audit

The IT auditor is concerned with the risks to the economy, efficiency and effectiveness with which the entity uses its resources in carrying out its responsibilities. To enable the IT auditor to make preliminary assessments on the risks to performance, he/she should gather information on the auditee’s aims and objectives (from mission statements, corporate plans, framework documents, annual reports etc.). The IT auditor will also need to identify the material IT systems (in terms of both their costs, and their contribution towards meeting business objectives).

Where IT systems are material the auditor should look for indicators of failing performance. These indicators may include:

- user dissatisfaction;
- unreliable systems;
- poor integration;
- escalating costs;
- delays in implementation;
- abandoned projects;
- high cost / slow maintenance; or
- disputes with providers.
Audit Risk in the Audit of Developing Systems

There is a risk that systems under development will not include the appropriate internal controls to ensure that the financial statements are free from material misstatement and irregularity, or that they will not operate in an economic, efficient or effective manner. The auditor can identify developing systems from IT strategy, expenditure plans, interviews with auditee’s personnel, Board and Steering Committee minutes. The auditor should ascertain what standards / methodologies the auditee is using to develop the systems. The auditor may need to carry out a more detailed review if:

- the system processes material financial transactions;
- the system is important to the auditee’s business; or
- the system involves significant amounts of money.

Evidence of poor management or development failures may be brought to the auditee’s attention immediately or left for a full scale value for money review at a later date.

8.4 Using Computer Assisted Audit Techniques

Auditors have long recognised that the power and speed of the computer can be harnessed to assist their audit work. The term “Computer Assisted Audit Techniques” denotes a series of recognised techniques we can use to help us conduct our audit in a more efficient and effective manner. CAATs generally fall into two separate categories:

- techniques for reviewing data; and
- techniques for verifying system controls.

Techniques for reviewing data

These involve audit examination of normal computerised accounting files and ledgers. These files may hold either transaction data or standing data in the form of master files. CAATs in this category are not confined to accounting data alone. They may also include techniques for reviewing non-accounting files such as system journals, recovery logs or data communication logs.

Some types of CAATs may be used for reviewing auditees’ data:

- audit enquiry software;
- audit sampling software;
- analytical software;
- embedded audit modules.
Techniques for verifying system control

In contrast to techniques which review data held within the system, CAATs under this category allow us to test the effectiveness and propriety of controls which operate within the systems. We can then assess whether key controls are operating effectively, judge how reliable they are and therefore determine how accurate the accounting and other records may be. Techniques which may be used to review and verify system controls and functions include:

- test data;
- integrated test facilities;
- parallel simulation;
- program comparison software;
- snapshots;
- mapping and tracing.

Uses of CAATs

These techniques may be used for a variety of purposes.

1. Substantive Testing

To gain assurance concerning the accuracy and propriety of an account by examining constituent transactions and records. In nearly all systems it would be neither practical nor cost-effective to examine large volumes of transactions and records. A sample is therefore drawn for audit examination. The computer can therefore be used to help draw a representative sample (i.e. that from which we can make the most accurate and valuable prediction concerning the whole population) as part of our substantive audit testing. In most cases the tests themselves are then performed manually once the sample has been drawn.

2. Compliance Testing

Certain types of controls (particularly those contained within application programmes and operating system software) cannot be effectively tested using standard compliance testing routines. For example, where it is not possible to observe the control in operation or interview the staff carrying out a check. Often there is no documentary evidence that the check was carried out - exception or error reports only being printed when a control failed, but no positive proof when the control has worked.

3. End-of-year Testing

These are normally of two types:

- checks related to and usually occurring solely on year-end routines;
- checks applied to verify final accounts figures.

4. Analytical Reviews and Predictive Analysis

This is a technique by which accounts figures are compared from year to year, or from figure to figure (e.g. by use of accounting ratios), after taking into account the movements in major
determining factors. In very simple cases such techniques can be applied manually, but more complex situations (with a number of interrelated but differently weighted factors involved) demand the use of computer supported techniques for the sake of efficiency.

5. Efficiency Analysis
A rather specialised branch of computer auditing, but nevertheless widely practised. It involves examination of the use made of a major asset - the computers. The aim is to ensure by an analysis of central processor and peripheral usage that an adequate throughput is being achieved for the minimum equipment expenditure. It may also be necessary to assess the effectiveness of resource allocation and possibly the charging of computer facilities across jobs to different departments.

6. Value-for-money Audits
This is a very wide and complex audit field in which many opportunities exist to use computer assisted techniques such as selecting a particular type of record (e.g. debtors over a certain age), the analysis of different components of an expenditure figure and relative trends over recent years. The examination of such records and trends may clearly highlight areas where value for money appears at risk or where an organisation is being wasteful. Other computer tools of use in value-for-money studies include:

- statistical analysis;
- survey techniques; and
- graphical presentation tools.
9. QUALITY ASSURANCE

9.1 Supervision and Quality Assurance

Audit records should provide evidence that team leaders have effectively supervised audit projects. Team leaders are also responsible for an appropriate level of technical advice. If particularly complex issues are involved the supervisors should possess, or be able to call on, an appropriate level of knowledge and expertise. Assignment Managers should be actively involved in:

- assignment planning;
- progress control; and
- review.

All audit work requires a combination of compliance with laid down procedures and the exercise of judgement. Review is an internal control which ensures that more than one level of judgement is brought to bear on the work carried out and the conclusions reached. It is concerned with both the quality and the efficiency of the audit and should confirm that:

- the original planned assumptions remain appropriate, taking account of significant events occurring after approval of the audit plan;
- the audit team have properly implemented the audit plan and have performed the audit in accordance with the appropriate Standards;
- the working papers adequately document the work performed by the audit team, particularly in areas where professional judgement has been exercised, and provide the basis for the conclusions expressed in the management letter or report;
- any significant findings have been brought to the attention of the auditee’s management, board of directors or audit committee.

9.2 First Stage Review

The Assignment Manager has prime responsibility for compliance with policies and Standards. To ensure compliance, the Assignment Manager should review all working papers in support of the audit and evidence this review. The Assignment Manager may delegate first stage review to a supervisor, but retains overall responsibility.

The reviewer evidences the review by initialling and dating each working paper, although this does not necessarily mean examining each working paper to the same depth. The level of scrutiny depends upon the nature of the area, its materiality, the entity risk and the complexity of audit judgements involved.

The first stage reviewer comments on any matters already identified as warranting attention, and adds any further points that require consideration by the Assignment Director. In each case the reviewer recommends appropriate action. Submission of the matters for attention should not be left until completion of the working papers if the matters for attention are important enough to warrant early involvement of the Director.
9.3 Second Stage Review

The Assignment Director should perform a review of the working papers in sufficient detail to be satisfied that:

- the audit has been conducted in accordance with appropriate Standards;
- the working papers contain sufficient and appropriate evidence to support the management letter or report on the computer information systems, particularly in areas where significant audit judgement has been used;
- the proposed management letter or report is appropriate and supported by the audit evidence.

In addition, the Assignment Director should review all working papers prepared by the Assignment Manager.

The extent of the Assignment Director’s review is a matter of judgement and will vary depending upon the experience and knowledge of the audit team, the complexity of the audit and the director’s assessment of the risk to the auditors. As a minimum it will normally include:

- the audit plan;
- the summaries of matters for attention and lead schedules on all working paper files;
- ensuring audit programmes have been completed and signed off;
- the evidence supporting all significant audit judgements;
- correspondence with the auditee;
- all original documentation produced by the Assignment Manager.

The Assignment Director evidences the review by initialling and dating all working papers examined. The Assignment Director bases the review on discussion with the Assignment Manager as to how the auditors have responded to key risks identified at the planning stage with the objective of ensuring that sufficient appropriate evidence has been obtained.

9.4 Quality Control Review

A quality control review is carried out after the completion of the audit and presentation of the report or management letter to the auditee. It is conducted by a manager or director who is independent of the audit team. The review focuses on key areas of professional judgement and compliance with Standards. Reviews are undertaken, often on a sample basis, to ensure that audit work complies with the relevant Standards and that sound judgements have been made.

Each review determines whether:

- the audit has been properly planned and identified risks have received adequate attention;
- conclusions on areas of judgement are explained in and supported by the working papers;
- any other opinion given is fully supported and documented in the working papers;
• the wording of the report or management letter points is appropriate in the circumstances and conforms to relevant Standards;

• the working papers meet the requirements of Auditing Standards in respect of documentation.

In the event of a disagreement between the reviewer and the auditor, both should meet with a higher ranked audit official to resolve the problem to the reviewer’s satisfaction. If agreement is not reached then the higher audit official should decide. Once agreement is reached, the working papers are signed off by those responsible for the decision.

The reviewer should be knowledgeable about IT audit and auditing standards. Where specialists have prepared a report it may be appropriate for specialists to review it on a peer review basis.

9.5 Communication with Auditees

Purposes of Communication

Auditors should communicate with their auditees, by appropriate means and at appropriate levels, at all significant stages of an audit. Good communications are necessary for the auditor to deliver an efficient and effective audit, they aid the auditee’s understanding of the audit process and they are the means by which the auditor helps achieve beneficial change in computer information systems.

Reporting to Management

The auditor should produce a report (or management letter) for management at the conclusion of each audit. If, during the course of the audit, a serious weakness or breakdown in systems controls is discovered, this should be reported to management without delay. Matters forming any part of a report to management must be based on reliable information collected in the course of audit procedures.

All reports to management should clearly state the scope of the work and therefore the limitations applying to any comments or recommendations which are made.

All reports should be produced promptly. A delay in communicating with management implies a lack of urgency, de-emphasises the importance of the matter raised and shows a lack of courtesy. The timetable for drafting, agreeing and issuing the report should be agreed with the auditee when the audit plan is finalised. Delivery should be timed so as to allow appropriate improvements in systems and controls to be completed before the next audit.

Recommendations in the report are usually developed from information that comes to the attention of the audit team. All audit staff need to be aware of the importance of the report and the opportunity it provides to improve financial management and accountability.

The collection of such information should not be left to the end of the audit. Every member of the audit team who identifies a matter should record the point on a separate collection sheet and in a style which is suitable for inclusion in the final letter.

In developing comments, it is important to focus on underlying causes of problems rather than simply to report the problems and their results. For example, the auditor should attempt to determine if errors are caused by lack of supervision, lack of training, insufficiently experienced personnel or systems problems.
The auditor must ensure that nothing is said that is inconsistent with the audit opinion or report. An exaggerated criticism may be irreconcilable with, for example, an unqualified opinion. A report should always indicate any corrective action that has been taken by the auditee as a result of, or since, the audit work.

**Input from the Auditee**

Frequently, management may ask to have certain comments removed or softened. Sometimes such objections have merit, but if the auditor continues to believe the comment is valid, it should be retained. In such cases the auditor would normally record management’s views along with the audit comments. Omitting a significant comment on the basis of contemplated corrective action is not acceptable. Also, where the auditee has corrected a problem which the auditor originally discovered, the auditor should still spell out the matter arising and action taken.

**Caveats**

For our purposes a *caveat* is a warning or caution given by someone to the effect that information is provided by them within particular constraints or for certain purposes. In other words, notice is given that liability will not be accepted for the actions of a party where those actions were beyond the scope of the information. It is usually essential that the auditor includes two caveats in the audit report:

- indicating the scope of the work; and
- that the report has been prepared for the use of management alone.

The auditor should avoid using caveats in the text of the report and should particularly avoid up-front summaries or introductions which consist mainly of caveats. It is satisfactory for caveats to be included as footnotes in small print. This does not diminish their legal meaning and gives the letters a more constructive tone.