Audit Manual – PART TWO
SISTEM BASED AUDIT

Table of content

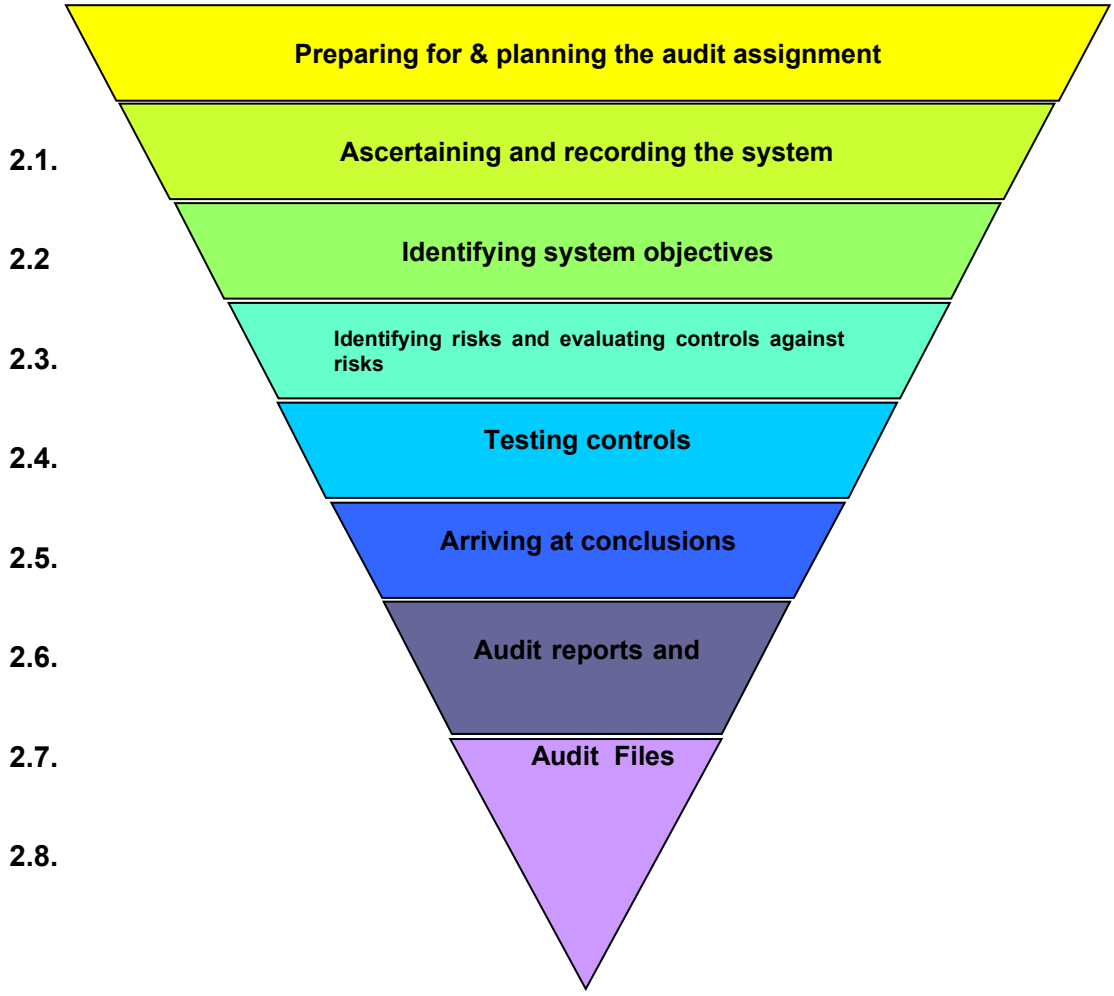
1. Introduction

This Section of the Audit Manual provides guidance on the Systems Audit approach which is one of the main audit methodologies applied by internal audit in the public sector in Macedonia.

All audit staff are expected to familiarise themselves with the procedures set out in the manual and to apply them in the course of their work. In some cases it may be necessary to adapt the procedures to reflect the situation in a particular organisation. Any such changes will be the responsibility of the relevant Chief Internal Auditor who will arrange for local guidance to be prepared and distributed.

2. Systems based audit

A systems based audit comprises the following stages:



2.1.Preparing for & planning the audit assignment

The preparing for & planning the audit assignment consists of: preliminary survey, organizing kick-off meeting and preparing an audit plan.

2.1.1.Preliminary survey

In a reasonable time limit before the audit is scheduled to take place a fact-finding exercise (preliminary survey) should be undertaken in order to get an overview of the area to be audited. This preliminary survey should provide the basis for planning the audit, and for determining:

a) The objectives of the audit;
b) The scope of the audit and any specific areas that are to be given emphasis because they are high risk, are of critical importance to the system and/or suffer from weaknesses which are already known;
c) Target dates for completion of each stage of the audit work;
d) Which auditors are to be employed on the audit and who is responsible for supervising the audit team and ensuring the quality of the audit work.

The preliminary survey will also establish the boundaries of the systems under review and identify any interfaces with other systems and any other audits which are planned. This provides the basis for drafting the Audit plan.

The preliminary survey should involve:

a) Review of the permanent audit file and previous audit reports, including reports from the State Audit Office;
b) Review of the strategic and operational plans of the area to be audited;
c) Current organisation charts;
d) Review of budget and management information;
e) Initial discussions with management of the organizational units to establish their objectives in the area to be audited;
f) Review of relevant legislation, regulations, instructions etc.

At this stage it is also useful to identify the goals and objectives of the area(s) under review and the key risks relating to those goals and objectives.

The review of previous audit reports is an important part of the preliminary survey. The reports provide an insight into the level of control at the time of the last audit, and an opportunity to establish whether or not agreed recommendations have been implemented by management.

2.1.2. Kick-off meeting

Prior to the Kick-off meeting a Letter of Autorization should be obtained, according to art.12 of the Rulebook of the basic elements of the Internal Audit Guidelines, Charter, Annual Plan and Programme of Internal Audit (published in the "Official Gazete Nmb. 38/05) (further in the text: the Rulebook). The template detailing the contents of that letter is provided in **Annex 4.2** to this section of the Manual.

Prior to the Kick-off meeting the internal auditors and external experts are required to have a Letter of Authorization, signed by of the Head of the Internal Audit unit, whereas the appointment of the Head of the Internal Audit unit, signed by the person in charge of the institution, prior to the performance of any of the audits within the Annual Plan. The Letter of Authorization shall specify: - Systems and procedures subject to the audit; - Objectives of the audit set out in the Annual Internal Audit Plan; - Audit team and Team Leader; and - Time-frame and deadline for submission of Final Internal Audit Report.

The formal start of the audit is the Kick-off meeting which should be held between the Head of the department to be audited and the Chief Internal Auditor accompanied by the Team Leader/Auditor carrying out the work. This meeting is intended to:

- Introduce the audit team to the management of the department to be audited;
- Outline the objective of the audit and give a brief overview of the methodology to be used – if this is the first audit of the department it will be necessary to give a more detailed explanation of the approach;
- Ask management to suggest particular areas which they think should be examined;
- Discuss areas which internal auditors consider on the focus of the audit;
- Explain that internal audit will keep them informed of the progress of the audit, and that management's assistance will be welcomed throughout the audit.
- Request additional information[1] about the business process under audit and agree on the list of documents required from the auditee;
- Distribute a copy of the Internal Audit Charter to all present on the Kick-off meeting (Form of the Charter in **Part** 1 from this Manual).

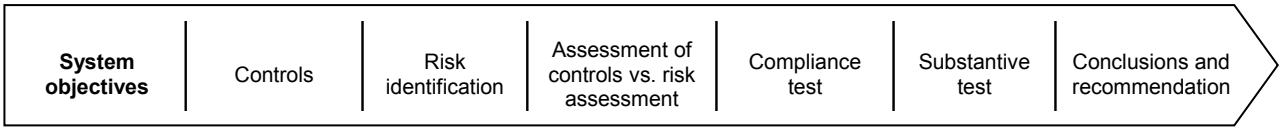
Some guidance on how to handle the kick-off meeting with management is given in **Part 3** of the Audit Manual.

[1] According art. 13, paragraph 2 of the Rulebook

2.1.3.Audit Plan[2]

After the preliminary survey and the kick-off meeting, an Audit Plan should be prepared. Template of the Audit Plan is given in **Annex 4.1** of this section of the Manual.

2.2.Ascertaining and recording the system



2.2.1.Purpose for describing the system

The main reasons for describing the system are:

- To confirm the auditor's understanding of the system formulating clear process / system objectives;
- To establish any interfaces between systems;
- To establish how the system fits within the Organisation;
- To provide a basis for assessing the extent to which internal controls prevent or detect and correct errors.

The description of the system forms the basis for the auditor's judgement, conclusions and recommendations. It also should provide basis for the evaluation of the strengths and weaknesses in internal control.

Because "describing" the system takes up a lot of time, exclude anything which is not significant to the audit.

The auditor should decide which technique or combination of techniques for recording systems (text and/or flowchart) is most appropriate, taking into account the nature and complexity of the system, the audit objectives and any audit work done earlier.

Sources of information can include:

- Files and papers from earlier audits;
- Organisational and procedural rulebooks, manuals, guidelines and other acts used in the organisation;
- Interviews and informal discussions with managers and staff (detailed guidance on interview techniques is contained in **Part 3** of the Audit Manual);
- Observation of the physical environment and the working methods used. It is particularly useful where no physical evidence that something has happened remains after the event. Remember that the presence of the auditor may influence the behaviour of staff and the practices observed may not, therefore, be typical. It may also be difficult to substantiate the evidence.
- Documents and records used in the system;

[2] The Audit Plan means the audit program according article 11 of the Rulebook.

- Reports prepared by any Control and Inspection Units;
- Any other reports relating to the area under audit;
- Management information.

2.2.2. Steps required in documenting systems

This section presents all the steps which are required in documenting system. If the system has previously been documented far less time will have to be spent in discussion with managers and staff. Similarly, if the system has not significantly changed. The steps are as follows:

1. Establish an outline of the system to enable you to decide on whether to use narrative or flowcharting to document the system, and also to decide which of the main sub-systems it will be appropriate to describe separately;

2. Obtain a detailed description of the systems and internal control features from discussions with departmental personnel. This should include a record of:
   - Which processes and procedures are carried out and by whom;
   - Any changes in procedures for different types or groups of transactions – eg those of high value;
   - Measures taken to maintain the continuity of the working process (lunch hours, holidays, vacations or peak flows of operations);
   - All documents used in the process;
   - All computer reports along with their purpose and the way they are used.

3. Record information on rough flowcharts or notes. If possible compare with acts describing internal procedures.

4. Perform walk-through tests (see below) to ensure that the system actually does operate in the manner which has been described.

5. Prepare documentation describing the system – narrative and/or flowchart.

6. Cross reference documents and reports of the system to the narrative and/or flowchart.

When documenting system, the internal auditor should remember that the volume of documentation should be limited to what is needed to identify and record the internal controls.

2.2.3. Extent of the systems description

This should be detailed enough to allow the user and the person reviewing the audit to understand how the system works and how internal controls are achieved. Depending on the objectives of the audit in some cases it may be necessary to record the complete system, and in others it may only be necessary to record key areas of the system.

When recording the system it is important to:

- Record the system as it **actually** operates;
- Identify and record all types of procedures and transactions covered by the system under audit (including exceptions such as national holidays, staff holiday periods, unusual overtime working hours etc);
- Look carefully for identifying controls - they may not always be clearly indicated;
- Record only the elements of the system essential to the audit;
- Copy only essential documents. Unnecessary copying of documentation can be wasteful and tends to make it difficult to review audit files;
- Remember that the description of the system found in such documentation may be out of date and incomplete.

If they provide adequate explanation, copies of standard documentation and significant reports or summaries may become part of the audit record. System records should also show the sources of information e.g. rulebooks, manuals, interviews.

2.2.4. Documentation of the system

Systems documentation normally takes the form of narrative descriptions, flowcharts or a combination of the two.

2.2.4.1. Narrative Descriptions

A narrative description helps to give a complete picture of the system. It provides a detailed record of the system under audit and, taken together with other forms of system records, it should cover:

- System objectives and targets;
- Links and interfaces with other systems;
- The environment in which the system operates;
- The allocation of authority and responsibility;
- All key controls and systems processes;
- Exceptional situations or cases that may need to be dealt with by the system;
- Ad hoc controls such as management reviews.

Narratives may cover detailed descriptions of transaction flows but in some cases these can be better recorded through flowcharts (see next chapter). It is often useful to use a combination of narratives and flowcharts – using flowcharts to describe more complex parts of the system. If flowcharts are used as well they and the narrative descriptions should be cross-referenced to each other.

Narrative descriptions may be usefully divided into:

- A summary overview of the system; and
- Separate detailed descriptions of the main constituent parts of the system.

Full use should be made of headings and they should be organised in a logical way in order to give a clear picture and make handling and updating easier. Wherever possible the source of the information and the names and titles of people interviewed should be recorded. A clear concise record of the system should be prepared. **Annex 4.3** of this section of the Manual.

2.2.4.2.Flowcharts

Flowcharting is a diagrammatic method of recording and describing a system, which shows the flow of documents or information and the related internal controls within a system. Flowcharts can help:

- To obtain a perspective on the whole system;
- Gain an understanding of the auditee's objectives;
- Identify segregation of duties;
- Help the person supervising the audit to identify areas which are not being covered by the audit.

Flowcharting is likely to be most effective if a logical, top-down approach is taken by starting with an overview or summary flowchart, followed by detailed flowcharts of specific processes if necessary.

There are various methods of, and symbols for, flowcharting. **Annex 4.4** of this section of the Manual sets out the symbols which should be adopted by all Internal Audit Units. Microsoft Visio (MS Excel or Word is also possible to use) provides a flowcharting facility and there are also a number of software packages available for producing flowcharts (examples of flowcharts are shown in **Annex 4.5** of this section of the Manual).

When preparing flowcharts remember:

a. Flowcharts are primarily designed to show document flows rather than operations – although other operations can be explained by means of narrative notes if necessary;
b. Try to avoid mixing up the 'regular' process and exceptional processes (two or three transactions per period) on the same flowchart. Prepare separate charts for the regular and the exceptional processes;
c. To consider whether it is better to record the system by preparing one or more basic flowcharts which show the main flows in the system - supplemented by narrative description where necessary;
d. To flowchart the actual system. In some cases it may be necessary to record the 'official' system , and in those cases the charts must be labelled clearly to show whether it is the official (prescribed) or the actual (real functioning) system;
e. To work in pencil. This will save time redrawing the flowchart when you make a mistake;
f. That each flowchart should have a title, the date of creation and of any amendments to it and the name of the person who drafted it;
g. To make sure that all documents (and every copy of each document) on the flowchart are fully dealt with;
h. To think carefully before preparing a flowchart. Ask yourself whether it's really necessary or whether narrative description will be just as effective and less time-consuming.

Flowcharting can be a very effective way of recording document flows in a system. Advantages of flowcharting are:

- Information can be easily communicated and assimilated;
- Flowcharts highlight the relationship between different parts of the system;
- The auditor can see the whole flow of documents: potential bottlenecks can be identified easily;

- Flowcharts offer a consistent method of recording;
- The auditor has to obtain a clear understanding of information flow in order to draw up a flowchart of a complex system;
- Cross-referencing between systems is made easier.

There are a number of disadvantages to using flowcharts. The most important is the time they can take to prepare. It is very easy for auditors to spend a lot of time preparing a flowchart when it would have been more efficient and useful to do a narrative description instead. Other disadvantages are:

- They are limited in scope and may not identify managerial and organisational controls;
- The technique and conventions have to be learned and practised;
- Complex flowcharts may confuse rather than clarify;
- The auditor usually needs some training and experience to be fluent in preparing them.

2.2.5.Other points to consider

2.2.5.1.Organisation Charts

The organisational structure relating to the system under audit should be recorded. A copy of an existing organisation chart will suffice, as long as it is accurate and up to date.

An up-to-date organisation chart will show details of the information flow, relationships in the organization and responsibilities. It is also useful in identifying staff and deciding where audit testing needs to be done. The date the chart was prepared should be recorded.

The chart may include:

- Main department/units with a description of their functions;
- Job titles, grades and names of staff together with lines of responsibility;
- All reporting lines.

2.2.5.2.Minimum Contents of System Documentation

Whichever method is used for documenting the procedures in each system there are certain items, which should be included on every system file. These are:

- Examples of documents describing their purpose and use. These documents and reports should be filed in the order in which they are used in the system, and cross-referenced to the narrative note or flowchart.
- Examples of reports (whether computerised or manually prepared) describing their purpose and use;
- Details of the number of transactions passing through the system. These are essential to a full understanding of the context of the system in relation to the overall activities of the entity. It is therefore necessary to summarise data such as:
  - Number of transactions;
  - Value of transactions;
  - Seasonal fluctuations.
- Forms used to evaluate the system.

It may also be useful for the auditor to know the number of employees or a stratification of the transactions by value or age to assist in the evaluation of risk when a weakness is highlighted.

2.2.6. Checking if the system is recorded correctly

It is important to ensure that the system is recorded accurately because it provides the basis for an evaluation of internal controls and for preparing a programme of audit tests.

If there is a lack of written procedures about processes in the public sector, please ask for confirmation of your narrative or flowchart, by signed from the manager of the audited unit.

2.2.6.1. Walk-through testing

In conducting 'walk through' tests, the auditor looks primarily for evidence of the existence of controls. This may involve examining a small number of different transactions at each stage of the process or following one transaction through from start to finish. The aim of this type of testing is to make sure that the system works in the way it is described in the systems narrative or flowcharts and to confirm the controls in place at each stage.

Normally transactions are followed from start to finish (final processing). However, sometimes it is more convenient and practical to start from completion of processing. It is important to consider documents, which pass through other minor systems and sub-systems outside the main system, and to look carefully at each file of documents and confirm where and why they are kept.

What to do with differences between the systems record and the walk-through tests?

When this happens there are two possible reasons:

- The system record you have prepared is mistaken, or
- The system record is correct but the system is not working properly.

If there is a difference, or any other information is identified which is inconsistent with the flowchart, you should refer back to the original source of the information before doing any more work. This is important because, if the system record has to be amended, the paths for walk-through test also may have to be changed.

When the difference is the result of an incidental breakdown in the system, you will normally need only to record this fact on your working papers. This information will then be taken into account in the evaluation of internal control.

2.2.7. Developing an Audit Programme

Once you have identified and confirmed the system/process or activity objectives the audit manager should start developing the Audit Programme (**Annex 4.7** in this section of the Manual). First step is to record the process objectives in column 1.

System objectives	Control objectives	Risks	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments
1	2	3	4	5	6	7	8	9

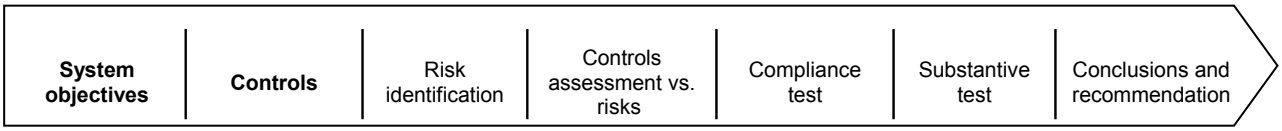
The purpose of this chart for the Audit Programme is to guide the auditor through the audit. It represents the main phases of the audit and gives frame to the internal auditor's professional

activities, decisions and conclusions. In case of complex process, or multiply audit objectives or control objectives, the auditor should prepare several charts or the main Audit Programme should be separated for each process, audit or control objective, as appropriate.

This chart is also an instrument for the management and quality control. Its content shows how well did the auditor understand the operations and process objectives; his capability to identify controls; risk awareness; level of knowledge to assess controls vs. risks and process objectives; ability to determent the extent of substantive and compliance tests, as well to create and carry out tests. The last column with Conclusions and Recommendation contains information about the results of the audit as a whole or specific step of the audit or procedure.

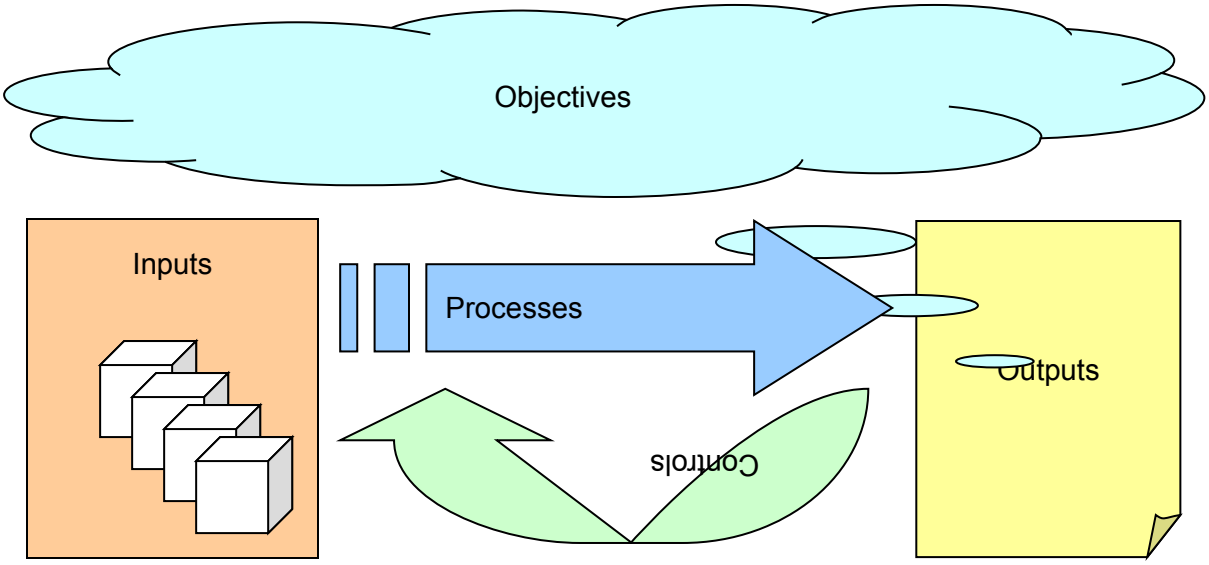
This chart is also useful for following the audit activities, so that anyone who is interested could become familiar with the audit process and check if the audit is carried out in compliance with the professional standards.

2.3.Identifying system objectives



The key to an effective system based audit is to identify the system objectives that determine the control objectives against which controls in the system can be audited.

A system has five main elements:



Each of these elements is explained in more detail in **Annex 4.6** of this section of the Manual. A systems based audit is concerned particularly with establishing the link between controls and objectives in order to gather evidence to support the auditor's professional opinion on the adequacy and effectiveness of internal control in that system.

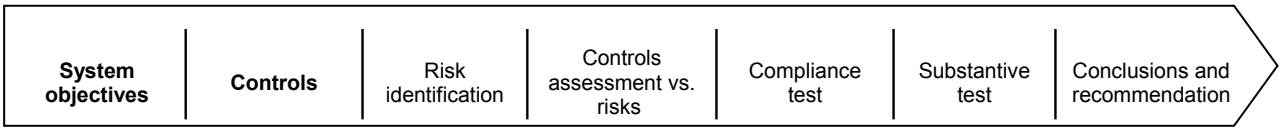
The first step is to identify the objectives laid down by management for the system. For example in a procurement system the objectives set by management might include:

- 'To ensure that the national law and legislation and EU requirements are met in placing procurement contracts'
- 'To reduce the cost of procurement by 5% each year for the next three years'
- 'To pay all valid invoices on time'.

System objectives such as these can be either, formal and written down, or informal. When you are trying to find out what they are, you should remember that in every system there will be a hierarchy of objectives - starting with those objectives set by senior management and working down to the objectives of the people involved in the detailed operation of the system.

By obtaining an understanding of what the objectives of the system are, it will help you to identify what the control objectives should be. The control objectives you set need to be consistent with the objectives of management in the organization, and should be discussed and agreed with management before you start any evaluation of controls.

2.3.1. Establishing control objectives



One useful way of thinking about this is to think about the organizational structure relating to the area you are auditing. This involves:

- identifying the main activities;
- determining the objectives of those activities or processes, and
- developing the control objectives which will help ensure the achievement of the objectives of the main activities or processes.

As a simple guide it may be useful to work on the basis of one control objective for each activity – although this rule should not be applied too rigidly.

For example with procurement the main sections/units involved could be: the department(s) requesting the supplies, services or works; the purchasing/contracts section; the department(s) receiving the goods or services and the accounts department.

For each of those sections or units you can then establish the activities which they carry out and this will help you to decide on the control objectives. So, for procurement:

- the *department requesting the supply* will be concerned with purchase requisitioning and (in many cases) receiving the supplies, services or works
- *purchasing/contracts section* will be involved in: purchase requisitioning; ordering; tendering and contracting; supplier database etc

- *accounts department* will be receiving invoices; validating and paying invoices; supplier payment files etc

Control objectives should include general control requirements such as:

- economy and efficiency
- prevention and detection of fraud and abuse
- reliability and adequacy of management information
- compliance with laws, legislation, management policies and rules
- security of assets, intellectual property and data
- the completeness and accuracy of the records and accounts of the organization.

An alternative approach to identifying control objectives is described by considering control objectives under the following categories:

- Organisation
- Authority
- Transaction recording and processing
- Asset recording and processing
- Security
- Verification

The following framework can be used to establish control objectives for most systems and processes which exist in each organization. For each area the framework lists a series of control elements. Against each of those control elements are suggestions for the possible focus of control objectives.

The framework needs to be used carefully and is intended for use as an aid to identifying control objectives. It is important to remember that different control objectives will apply in different systems. **It should not be regarded as a comprehensive list of control objectives** and auditors should be constantly thinking about additional control objectives to reflect the particular context in which a system is operating, and any specific problems facing the system or process under review.

Framework for control objectives

2.3.1.1.Organisation

Control element	**Possible coverage of control objective**
Guidance and direction	- services, total number of employees and by departments/units, are in accordance with the organisation's policies
Rules and procedures	- Rules and procedures for incurring expenditure, collecting income and the custody and disposal of assets are in accordance with the organisation policies.
Relevant & subject to review	- Acts for systematization are regularly reviewed and approved by the appropriate level of management.

2.3.1.2.Authority

Control element	**Possible coverage of control objective**
Statutory authority	- services and transactions are in accordance with legislation and other legal requirements

Professional authority	-	Quality of service provision is in accordance with professionally recommended standards.
Organisation authority	-	scales of charges for services etc are regularly reviewed and approved by the Governing board / Municipal Council or the appropriate level of management.

2.3.1.3.Transaction recording and processing

Control element		**Possible coverage of control objective**
Occurrence	-	recorded income and expenditure did in fact occur.
Completeness	-	all transactions have been processed and recorded in the accounts or permanent records as appropriate.
Measurement	-	transactions have been valued in accordance with the laid down accounting policies.
Timeliness	-	transactions were initiated or recorded within a reasonable timescale.
Regularity	-	transactions and activities have been carried out in accordance with appropriate regulatory authority.
Propriety	-	Fairness, integrity and transparency have been observed in the negotiation of the contract for the services or supply.
Presentation and disclosure	-	each transaction is coded correctly. (On completion of the annual financial statements, that the form and content of the statements are in accordance with appropriate accounting standards and regulations)

2.3.1.4.Asset recording and processing

Control element		**Possible coverage of control objective**
Ownership	-	recorded assets are owned by or attributable to the organisation.
Completeness	-	all assets are recorded in accordance with standing orders and financial regulations.
Valuation	-	recorded assets have been valued in accordance with the organisation's policies.

2.3.1.5.Security

Control element		**Possible coverage of control objective**
Assets	-	access to prime documents is properly authorised.
	-	all assets are secure and custody clearly stated.
	-	access to assets and asset utilisation is properly authorised.
Permanent records	-	permanent records are secure and custody clearly stated.

2.3.1.6.Verification

Control element		**Possible coverage of control objective**
Permanent records	-	recorded assets are physically checked and the need for write off provisions assessed.

- recorded information is periodically compared with prime data or checked physically (census).

Control objectives should relate to the particular nature and operation of the activities which are needed to meet the specific objectives of the system. They should also be specific and show the purpose of control - and not the control itself. For example:

- in a purchasing system one control objective might be 'to ensure that invoices are paid only for goods or services which have been received'
- in a payroll system a control objective could be: 'to ensure that payments are made only to valid employees of the organization'
- in a security audit a control objective could be 'to make sure that only accredited staff and visitors are permitted to enter the building'.

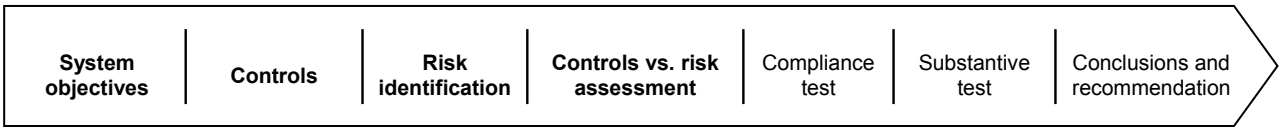
Some examples of control objectives for some common systems audits are provided in **Annex 4.9** of this Manual.

2.3.2.Recording control objectives

Process objectives	Control objectives	Risks	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments
1	2	3	4	5	6	7	8	9

Once the auditor has determined the control objectives they should be recorded in Audit program (column 2). This Audit program will be filled gradually for each step of the audit.

2.4.Identifying risks & evaluating controls against risks



2.4.1.Headline risks

It is often very useful to identify the 'headline' risk(s) associated with each control objective and to record them. This ensures that the auditor is clear about the context in which the control objective is set, and that the record of the system or activity remains within the parameters of the control objective. It can also help to reduce the amount of time spent on the systems description. Some examples of 'headline' risks include:

- damage to the reputation of the organisation or a particular department within the organisation
- a major security breach through unauthorised access to computer facilities
- fraud

The next stage of a Systems Based Audit is to identify and evaluate controls which exist to lessen the risk of failing to achieve a particular control objective. The key elements of this are:

- deciding on the risks relating to each control objective
- identifying the actual controls which exist in the system
- evaluating the effectiveness of those controls.

2.4.2.Identification of risks

Once you have identified the system it is useful to consider whether you need to add in further control objectives to those you identified at the start of the audit. As before, these should be recorded. Risks should be identified and recorded for each control objective (column 3 in Audit program). This will make it easier to decide the type of testing and how much testing needs to be done.

Process objectives	Control objectives	Risks	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments
1	2	3	4	5	6	7	8	9

The risk endangers the achievement of the objectives defined for the process. During the execution of the processes many errors may emerge. These may be unintentional errors (misunderstandings, confusions, lack of competence etc.) but also intentional errors (varying from deliberate wrong application of rules to abuse like forgery and misappropriation usage of means). Such risk can be identified on the basis of the information collected at an earlier stage. The auditor shall estimate the risk at the planning stage and during the audit itself.

Risks are classified according to two criteria:

1. the probability for a certain risk to appear in reality;
2. its impact, which can be identified by the following table:

Classification of risk			
Impact ***Probability***	LOW	MEDIUM	HIGH
HIGH	Medium	High	High
MEDUIM	Low	Medium	High
LOW	Low	Low	Medium

Risk shall be classified as:

- **Low –** there is a low probability that the identified risks will have a negative impact on the audited body;
- **Medium –** there is a medium probability that the identified risks will have a negative impact on the audited body;
- **High –** it is probable that the identified risks have a negative impact on the audited body.

The answer to the question whether the impact of a given risk should be qualified as low, medium or high, is based on a competent opinion formed by the auditor. The possible factors (characteristics, features, qualities) having a role here are the established priorities and the implementation of the policy, the potential image risk and the financial interest related to them. The calculation whether the manifestation of a certain risk is probable or not, is a result of the professional judgement of the auditor. The complexity of the audited process and the leadership and administrative framework in which the process develops are the significant factors in calculating the likelihood impact of a given risk.

It is recommendable that the auditor discuss with the management of the audited body the risks identified by him and their classification, so that no risk factors are left out and to avoid unnecessary differences between the auditor and the management with regard to the process. The auditor should predominantly concentrate on the high risk areas.

Some typical risk categories are:

- **Error** – is there a possibility an error could occur during the process in question or that information held in a key data file or store (ex. details of supplier; employee records) could contain errors.
- **Fraud –** could the process or information be deliberately manipulated for personal gain which might go undetected.
- **Theft** – in the delivery of the systems objectives and the performance of the activity under review are there physical assets which someone could remove for personal benefit.
- **Regulatory** – could the process or system not be compatible to international, European and national and any rules and regulations laid down by the central government or the municipality.
- **Disclosure** – is there a possibility of unauthorized disclosure of information or of the way in which the system or process operates which might lead to loss, embarrassment or other disadvantage.
- **Disruption** – is there a possibility of loss or disruption which would make it difficult or impossible to operate the system or process or could lead to the loss or corruption of data.
- **Value for Money (VFM)** – is there the possibility of uneconomic, inefficient or ineffective use of resources in the performance of the process or system.

Example for identification and risk assessment in the public sector is given in **Annex 4.8.** of this section of the Manual.

2.4.3. Identification of key controls

For each risk, using the description of the system you prepared, you should then identify the control or controls which are intended to manage that risk. Full details of the control should be recorded in column 4 in Audit program. It is important that you record the actual controls in existence, and not the ideal controls for the situation, or the controls that management would like to have in place. Details should also be included of who (grade and position) performs the control, and where.

Process objectives	Control objectives	Risks	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments
1	2	3	4	5	6	7	8	9

Controls are actions and procedures established by the auditee to ensure that the objectives of a system are met. Even if objectives are met without controls, reliance cannot be placed on any system which functions without adequate controls.

More information on the different types of control is provided in **Annex 4.9** to this part of the Manual.

2.4.4. Evaluation of controls

Evaluating controls involves two stages:

- evaluating the system design to establish the **adequacy of control**, and
- evaluating the operation of the system to establish the **effectiveness of control**

2.4.4.1.Evaluation of the system design (adequacy of control)

This is done after the system is recorded. The auditor must consider whether the control objectives will be achieved by the identified controls. This requires the use of audit judgement. This preliminary evaluation of the adequacy of the existing controls involves:

- starting at the higher level controls (e.g. planning and risk management) and working down to lower level controls over individual transactions
- considering the probability that something will go wrong and the significance (materiality) to the organization if it does go wrong
- looking for compensating controls which may enable the control objective to be met
- looking for unnecessary controls, or ones which cost too much to apply.

It is necessary to establish whether the controls will, under reasonable circumstances, prevent and/or detect and manage risks/errors. If they will prevent and/or detect risks/errors, the auditor should record this conclusion in column 5 of Audit program. It will then be necessary to test the actual operation of the controls. Column 6 and 7 is for the reference to the relevant Audit Test Record.

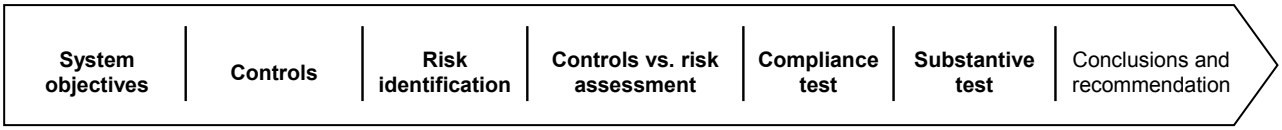
Process objectives	Risks	Control objectives	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments
1	2	3	4	5	6	7	8	9

If the control will not prevent and/or detect errors etc, or if there is no control at all this should be recorded in column 9 on Audit program (comments on the nature of errors or weaknesses). The auditor will not normally test those controls which are considered to be inadequate, but may - in extreme cases - conduct substantive tests to identify and quantify the extent of any errors. Internal Control Questionnaires can be used to aid the identification of strengths and weaknesses of controls.

2.4.4.2.*Evaluation of the operation (*effectiveness*) of the* system

This involves testing to ensure that the controls which have been identified have been operated as intended and that they are achieving the control objective. This is dealt with in next chapter of this manual.

2.5.Testing controls



2.5.1.Why is it necessary to test?

It is management's responsibility to ensure that the systems of control are adequate and that they are being complied with. This means it is for management to carry out appropriate checking or testing procedures to ensure that laid down procedures are being complied with, assets are safeguarded, financial records are maintained etc. Under no circumstances should internal audit be seen as part of this internal check system.

Audit testing is a supplement to management's own testing, and is an essential part of the independent appraisal of internal control carried out by internal audit. This testing:

- confirms that management has been carrying out checking and testing, and
- detects violations which management may not have identified.

Audit testing can be a very substantial part of the audit process, sometimes taking up to half the time available for the audit. This means it is important to ensure:

- audit tests are carefully planned
- there is adequate evidence of the testing which has been done
- conclusions can be fully supported by the testing done.

Internal auditors use testing to evaluate the operation of the system and to form or corroborate an opinion about the adequacy or otherwise of control. This is done by measuring particular characteristics of selected transactions or processes and comparing the results with those expected. For example, the control should assure that in the financial report for some specific year are included only data for transactions performed that year, and not for transactions from previous or future years.

There are two main types of testing: test of controls or compliance test and substantive testing.

2.5.2.Compliance testing

Compliance tests aim at collecting evidence whether the control procedures are correctly implemented and are reliable. Compliance tests are performed to guarantee the effectiveness of the functioning of internal control measures throughout the control period (here the control shall be also oriented towards finding the existence of the respective control measures). These activities shall provide evidence for the auditor to affirm the functioning of the control measures. The purpose of compliance tests (i.e. testing the control mechanisms and procedures) is to confirm that the existing control procedures are correctly applied and are reliable.

The main purpose of compliance tests is not to identify errors, deviations or potential fraud, but to identify the control procedures, which are not performed correctly. The reasons for the

omissions and deviations are more important to the auditors than the omissions and deviations themselves.

To find out the performance of internal control measures, you should carry out **compliance tests** through partial observation of selected cases, events or items. In practice this usually is a combination of compliance tests and detailed tests.

The number of compliance tests carried out depends on two factors:

- the size of the information flow related to the respective process;
- the nature of the control measures.

You should estimate whether the control procedures were adequately performed during the audited period. The planned tests shall be evenly distributed in time.

If one or more similar deviations are found, you should trace out the risk of these deviations and whether this risk is sufficiently covered. If the measures are insufficient to cover a certain risk found, this has a reflection upon the identification of the residual risk. Of course, a considerable number of deviations will make you adapt your opinion of the quality of the internal control system. In such case the planned number of detailed tests shall be increased.

Further information on how to plan, design and evaluate tests of controls is provided in **Annex 4.11**. to this part of the Manual.

2.5.3. Substantive Tests

Where it has been determined, through compliance testing that they are weak or inadequate controls you may decide to conduct some direct substantive testing. The purpose of this is two fold:

- to determine if any significant losses have occurred, and
- to contribute towards internal audit's assessment of the organisation's overall control environment.

The results of this work will either:

- provide assurance to management that there has not been any significant losses, to the organisation as a result of a weak control environment, or
- provide evidence to management that the weak control environment has lead to significant losses, and thus prompt management to take appropriate action

The objective of substantive testing is to evaluate the adequacy and completeness of outputs rather than the operation of controls. For example, checking the amount actually paid to a supplier is the same as the amount on the invoice and on the purchase order.

It is thus more detailed in its nature, more time consuming, and requires larger samples to gain the same level of assurance. However, errors discovered in substantive testing are more significant, as they usually represent a loss to the organisation, where as errors from

controls test demonstrate a control failed to operate – but not necessarily that an error occurred.

Annex 4.10. to this part of the Manual presents the steps in the decision making process when deciding on the type and extend of Compliance and Substantive testing.

2.5.4. The test program

Before starting any testing you need to decide:

- what to test
- what each test is for, and
- how to test.

When designing the test it is very useful to try to structure one test to cover a number of different control mechanisms and risks. For example:

- when testing the controls over purchase orders you could structure a test to allow you to verify several controls, including the authorisation of purchase orders (signatories etc); changes to purchase orders; and the controls over the receipt of goods and services purchased (details on purchase orders of quantities, prices, delivery dates etc)

- when testing controls over the authorisation of changes to standing payroll data you might structure a test to cover the addition of new employees (including verification of pay rates) and changes in pay rates for current employees (ex. on promotion).

Examples of Compliance and substantive tests are given in **Part 4** of this manual.

The following steps are to be performed in the field work (testing) phase:

- The detail of each test carried out should be recorded on a separate working paper (Annex 4.12. to this part of the Manual).
- Test results should be used for the Record of Audit Findings (**Annex 4.13**. to this part of the Manual).
- All tests and record of audit findings should be referenced in column 8 of the Audit Programme.
- Finally the most important findings, conclusions and recommendations should be summarised in the Audit Findings Summery Form (**Annex 4.14.** to this part of the Manual).

Process objectives	Control objectives	Risks	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments
1	2	3	4	5	6	7	8	9

2.5.5.Sampling techniques

In order to reach a judgement on the effectiveness of the internal control system adequate tests need to be performed on the system. If the review of the system and the walk-through tests indicate a weakness in the system, then further tests may be conducted to determine whether that weakness has been exploited and to what extent. The review of the system will also highlight a number of critical controls which appear to be operating effectively, but which need to be tested to ensure that they can be relied upon.

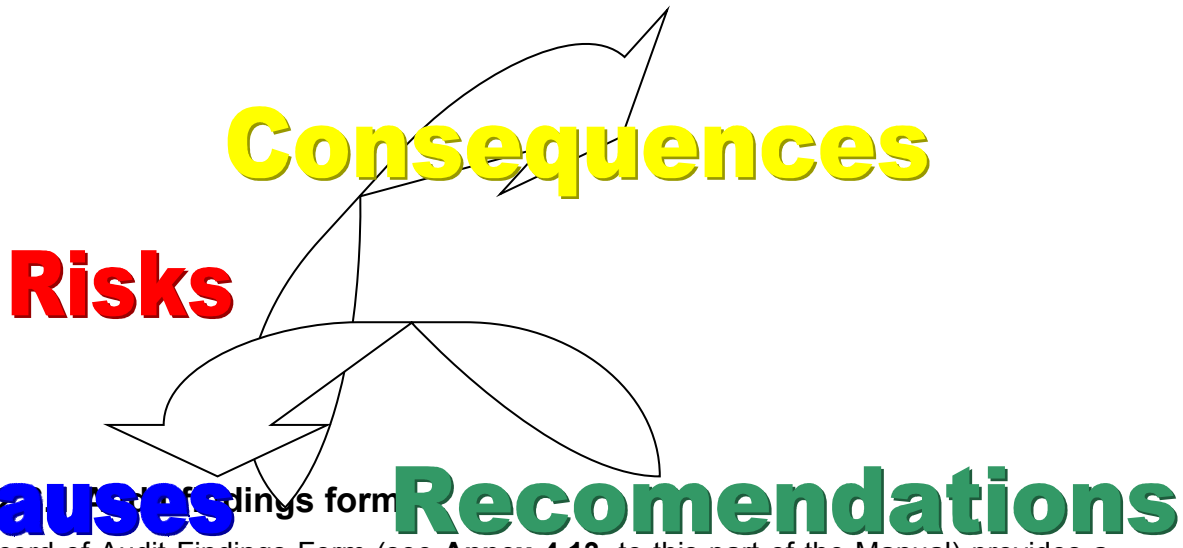
In order to carry out these tests on these controls it is necessary to use sampling techniques to determine a sample from the population of the system being audited (ex. purchase invoices in a procurement system). Clearly if you want to establish the adequacy of controls in that system the ideal approach is to test every purchase invoice, but this is nearly always impossible to do and it can be prohibitively time-consuming and expensive. Some guidance on different sampling methods and when to use them is given in **Part 3** of the Audit Manual.

2.6.Arriving at conclusions

System objectives	Controls	Risk identification	Controls vs. risk assessment	Compliance test	Substantive test	Conclusions and recommendation

This is the stage of a system based audit where the auditor considers the results of previous work before reporting to audit management and to the management of the area audited. It is important that you think about your findings and conclusions throughout the evaluation and testing processes.

Process objectives	Control objectives	Risks	Controls	Control evaluation	Compliance Test	Substantive Test	Working Paper	Conclusion Comments



The Audit Findings form

The Record of Audit Findings Form (see **Annex 4.13.** to this part of the Manual) provides a useful structure for handling the information you have obtained and to think things through in a logical way when writing the audit report. It is designed to help the auditor to establish the causes of the issues or weaknesses which have been identified from the evaluation of the system of control, and to develop suitable recommendations.

It should be completed as testing is being done and the nature and significance of control weaknesses are established. Wherever possible try to group related weaknesses together on the Audit Findings Summary Form (see **Annex 4.14.** to this part of the Manual). This will make it easier to plan your audit report.

2.7.Audit reports and action plans

See **Part 3** of the Manual

2.8.Audit Files

The working papers and any other documentation related to each audit assignment should be held on dedicated audit files. Those files should be structured in a clear and logical way in order to make it easy for anyone to find what they need and to understand what has been done, and why. The files can be held in electronic or paper form.

Appropriate use of indexes and of cross-referencing between documents and sections of the files is vital if documentation is to be accessible and assist the auditor to carry out the audit efficiently. This will also help anyone using or reviewing the files to follow the steps taken during the audit and to understand how conclusions were reached.

Maintaining well organized and structured audit files:

- enables the audit to be conducted in a logical manner
- helps ensure comprehensive coverage
- aids understanding
- makes it easier to identify weaknesses and draw the correct conclusions
- enables progress and findings to be readily reviewed
- makes report drafting easier
- facilitates the location of papers
- provides a formal record of the work undertaken.

Two types of file should be maintained for each audit - the Permanent File and the Current File.

The Permanent Audit File - contains all the ongoing information about the system, unit or department under review. The permanent audit file should be reviewed by the Auditor at the start of each new audit of that system etc. It should also be updated at the end of the audit.

The Current Audit File – contains all documents or information that refers to the current audit. It contains a detailed history of the current audit from determining the scope and objectives through to the completed Action Plan. It is advisable to create this file at the start of the audit and, as far as possible, to build it up during the course of the audit.

A suggested structure for each of these files is given at **Annex 4.15.** to this to this part of the Manual.

3. Supervising audit assignments

3.1.Responsibilities of the Chief Internal Auditor

The Chief Internal Auditor (CIA) is responsible for ensuring that individual audits are adequately resourced and properly supervised throughout. When considering resources care should be taken to ensure that the appropriate range of knowledge, skills and experience are allocated, and that the necessary level of supervision is provided. The level of supervision needed will depend on the proficiency and experience of each auditor and the difficulty and sensitivity of each assignment.

Other key areas on which the Chief of the Internal Audit Unit (CIA) should focus include:

- providing suitable instructions at the outset of an audit and approving audit objectives and work programmes
- making sure that work programmes are carried out, unless changes are both justified and approved
- making sure that audit reports are accurate, objective, clear, concise, constructive and timely
- ensuring that audit objectives are being met within allocated resource budgets and by agreed target dates as far as possible
- ensuring that laid down standards and procedures are being applied and that appropriate audit techniques are used.

3.2.Audit preparation

At the start of every audit the CIA and the Auditor or the audit team should discuss and agree;

- the scope and objectives of the audit - and whether any preliminary work is needed before the audit can start
- audit approach and techniques to be used
- the staffing of the audit
- a time plan for responsibilities of Auditors indicating duration, completion of the audit, etc
- administrative arrangements, security procedures, travel time, subsistence, locations, etc.

The CIA should brief the auditor or audit team before the audit starts to ensure that audit objectives are understood by the team and make sure that all relevant documentation and background material is assembled. The briefing should include approach and techniques, allocation of tasks to individual auditors, liaison with line management, reporting and administrative arrangements. Details of the briefing should be recorded in the Current Audit File.

3.3.Arrangements for the audit

The CIA should inform line management of the purpose of the audit and the timing and duration. If part of the audit testing strategy requires an unannounced visit (ex. a surprise cash count) the Head of Department should normally be informed on arrival.

At the start of the audit, the CIA and the Auditor should arrange an Opening Meeting with the line managers responsible for the work to be audited, and explain the audit task and the systems or activities to be examined.

Any requests for audit to look at matters not covered in the work plan should be referred to the CIA for decision. A provisional timetable and a final discussion date should be agreed. Periodic meetings may be arranged as the audit progresses, particularly where it is a long or complex audit.

3.4.Supervision of the audit

Supervision involves monitoring staff on assignments, reviewing their work, developing their skills and making sure that performance is in line with standards and work plans. More supervision is needed where a trainee is being used or if an auditor has a low level of skills in, or experience of, the type of assignment to which he or she has been allocated. The CIA should:

- review performance and progress periodically. This should include regular meetings with the Auditor(s). Failure to exercise control may result in objectives not being achieved or loss of direction and efficiency
- consider the actual man days spent on each audit and determine reasons for variances. The implications for future plans should be considered and any necessary action taken
- pay scheduled and unscheduled visits to see the auditor/audit team at work to assess the way in which the audit is being carried-out and the expertise which is being applied. They should note any training needs arising during the audit.

3.5.Review

This is an integral and continuous part of the audit process. All work should be reviewed by the CIA on an ongoing basis throughout the audit. Completed working papers should be inspected to ensure that they meet laid down standards and are relevant to audit findings and conclusions. It is also important to ensure that evaluation and testing are appropriate to the system which is being audited.

The extent of review will vary with the experience of staff and the nature of the assignment but it should be such that the CIA can be satisfied that the conclusions are sound and are demonstrably supported by relevant, reliable and sufficient audit evidence. There should also be evidence that all elements of the plan have been satisfactorily achieved and that the audit file has been reviewed by the CIA.

3.6.Continuous improvement

On completion of each audit the CIA should sit down with the auditor/audit team to assess the way the audit has been done and how effective it has been. This review is to establish 'lessons learned'. The review should ask:

- what was done well?
- what did we do badly/less well?
- what improvements could be made?

In the light of these reviews the CIA should consider whether there is a need for additional guidance on future audits, whether there are any implications for other audits and the effect on audit plans. Possible solutions to the problems identified could include staff training, better planning, the use of other audit techniques, a different approach to the audit etc.

3.7.Audit review record

A record of the reviews carried out should be prepared and held on the audit file. This record should show:

- the main stages in the audit and the major documents reviewed
- the results of the reviews
- who carried out the reviews
- the dates of the reviews
- lessons learned for the next audit

The review record should be signed by the CIA or other person reviewing the audit on completion of each stage of the audit. The exact timing of each review will depend upon the nature, complexity and length of the audit.

A sample of an Audit Review Record is in **Annex 4.16** to this part of the Manual.

4. Annexes

1. Audit assignement plan
2. Form – Authorization letter
3. Narrative description template
4. Flowchart symbols
5. Flowchart example - (vertical and horizontal type)
6. Key elements of systems
7. Audit program
8. Methods of identifying risks
9. Types of control
10. Decision points in a system based audit
11. Planning and performing tests of control (compliance tests)
12. Test record
13. Record of Audit Findings
14. Audit findings summary form
15. Structure of audit files
16. Audit review report

4.1.Audit assignment plan

Audit assignment plan	
Number and name of the audit according to the Annual Audit Plan	
Chief of audit team	
Revised organization	
Chief of the revised organization	
Revised systems or processes	
Key Business/System Objectives	1. 2. 3.
Short description of the system/process	
Important findings for the revised system/process from previous audits	
Key contacts **(list of people that will be contacted/interviewed)**	• • •
Audit Objective	1. 2. 3.
Audit Scope	
Priorities / key issues & possible problems	
Approach & audit techniques **(types and levels of research and testing: procedures for internal audit that refer to summarizing, analysing, proceeding and documenting data)**	
Audit team members (including outside experts and their tasks)	
Target Completion Date: **(Broken down into key stages)**	- preliminary research; - terrain work; - preparing draft report; - submitting provisional report; - submitting final report.

Prepared by: Approved by:

_____ _____

4.2.Form – Authorization letter

Based on Article 26, point 1, from the Law for Internal Auidt in the Public Sector (‘‘Official Gazette of RM“, Nr.69/04) and Article 12 from the Rulebook for basic elements of the Work Manual, charter, annual plan and program for internal audit (‘‘Official Gazette of RM“, Nr.38/05), chief of _____, issues the following

A U T H O R I Z A T I O N

Authorized is/are:

_____, _____ - Chief of Audit team;
(name and surname) (title)

_____, _____ - Member of Audit team; and
(name and surname) (title)

_____, _____ - Member of Audit team;
(name and surname) (title)

to perform audit of _____.
(systems and processes that will be subject of the audit)

Audit goals are _____.

The audit shoud be performed in the preiod from _____ 200_ year until _____ 200_ year, and the final audit report to be performed latest by _____ 200_ year.

CHIEF OF _____,

_____
(signature)

(Stamp)

4.3.Narrative description of system

The table shown below is only as model for text description. Internal auditor has to use format that will be easy to understand for the user, through increasing the space for writing or using blank form. Main rule that should be followed is: simply, shortly and clearly without unnecessary information.

Description of System / Process

Name of the system / process:	

Name of activity (step of the process):	
Description of the activity and related connected to it	
Name of the responsible person for the activity:	

Name of activity (step of the process):	
Description of the activity and related connected to it	
Name of the responsible person for the activity:	

Name of activity (step of the process):	
Description of the activity and controls connected to it	
Name of the responsible person for the activity:	

Date: …… **Prepared: ……..**

Supervisor: …….

4.4.Flowchart symbols

Flowcharts are used as a visual method of both manual and computer process analysis. Through visualisation, flowcharts can make it easier to understand how the system works than a detailed description would do.

Internal audit uses flowcharts mainly in preliminary studies and when scrutinising an internal control system. They can also be useful in developing new systems and for assessing whether your recommendations to improve procedures and systems are appropriate.

Flowcharts consist of symbols, each with a specified meaning, a brief explanatory text and connecting lines. The extent of any explanatory text depends primarily on the complexity of the processes and on who is going to use the flowchart.

Various levels of flowcharts may be used depending on how detailed they are; the number of levels corresponds to the complexity of the systems and/or procedures depicted. The number of levels of a flowchart should be adequate so as to clearly and precisely depict the individual parts of the flowchart and their corresponding links in their complexity. As a rule, at the top of the hierarchy the flowcharts depict the system as a whole. Each following level below depicts in greater detail one or more parts depicted on the level above.

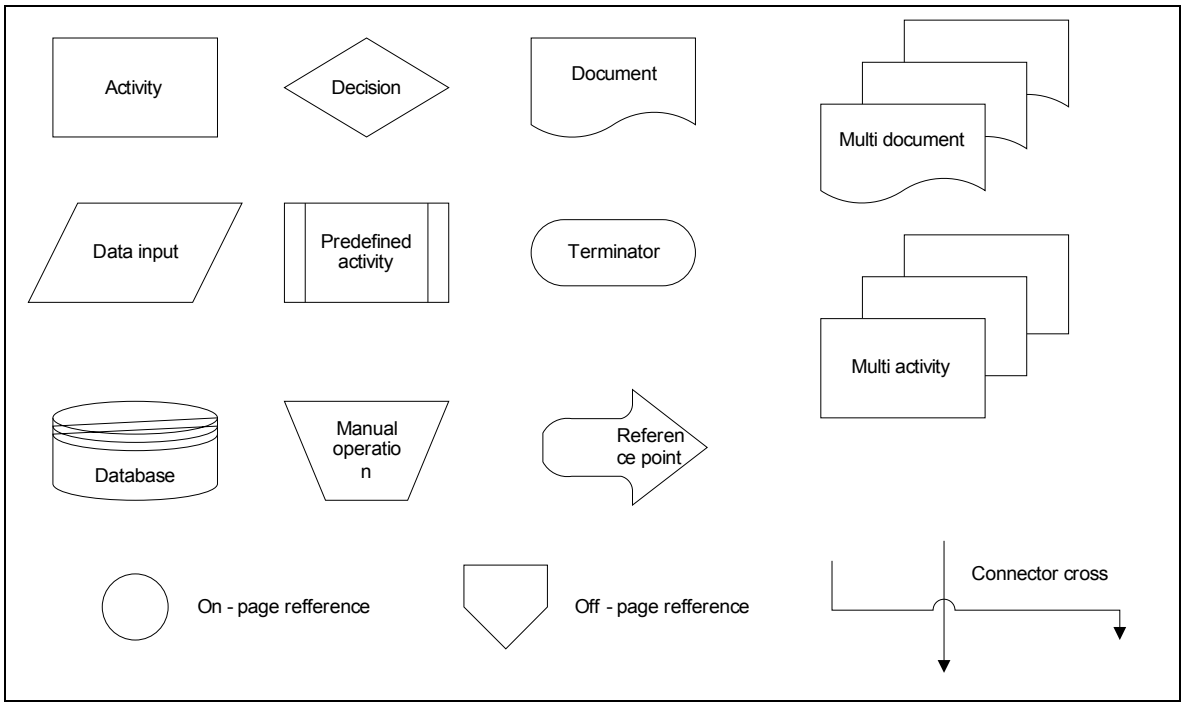
4.4.1.There are two main types of flowchart:

1. **Horizontal flowcharts** (system flowcharts) describing the horizontal distribution of responsibilities (units, positions) rendered using columns
2. **Vertical flowcharts** depict the hierarchical sequence of measures.

When carrying out your audit you need to decide which is the most appropriate type to use.

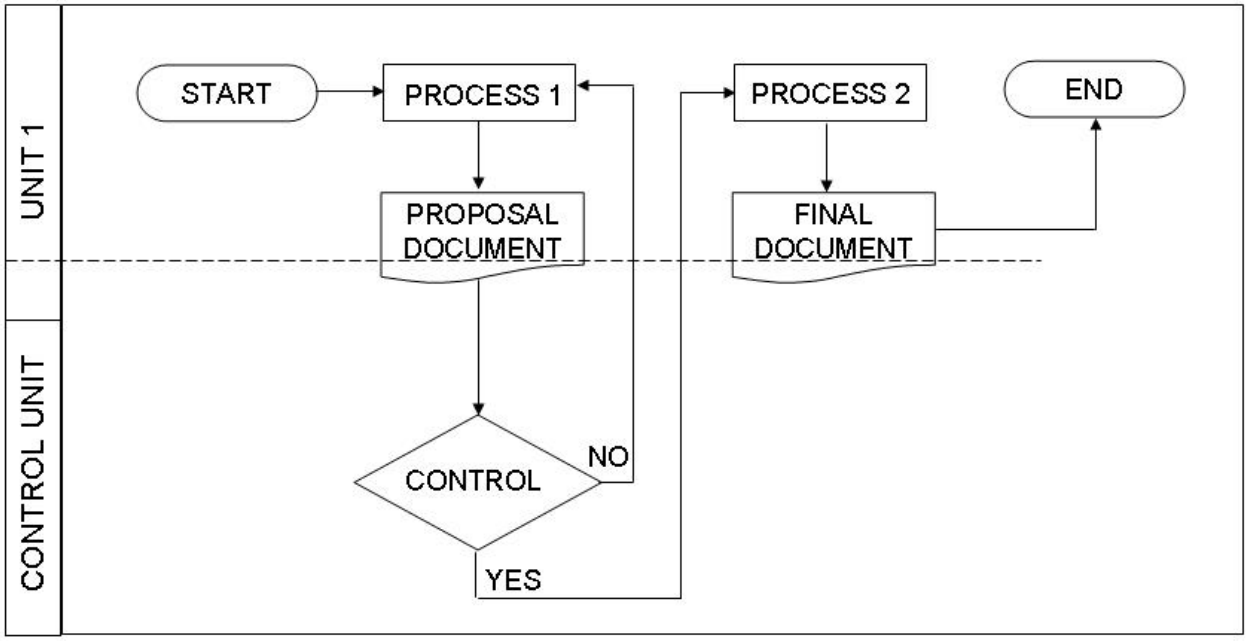
Standard flowchart symbols are given and easy to be used in Word, Excel (Draw-AutoShapes-Flowchart). Most often used program for drawing flowcharts is Microsoft Visio.

The following diagram shows the principal symbols which should be used.

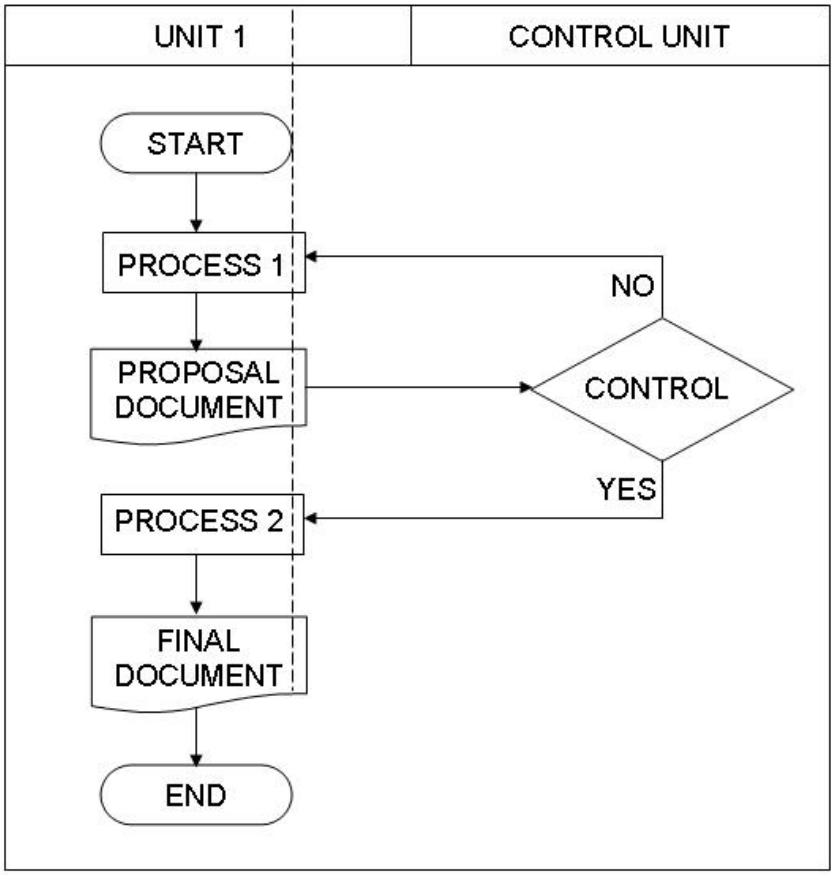


4.5.Flowchart example (vertical type and horizontal type)

4.5.1.Vertical flowchart



4.5.2.Horizontal flowchart



4.6.Key elements of systems

Every system has a number of key elements which are:

objectives/targets

▼

inputs (resources)

▼

processes

▼

controls

▼

outputs (results)

OBJECTIVES

They are key to any system. They set out what the unit, department or process is trying to achieve. At the highest level they set out the aims of the organization (e.g. to increase tax collection rates by x%); at a lower level they should relate to individual activities or processes (to raise revenues from excise duties on alcohol by x% by end 2005). Good objectives generally should have the following characteristics:

- **S**pecific
- **M**easurable
- **A**chievable
- **R**ealistic
- **T**imescales

INPUTS

These are the resources which feed the system either for conversion during processing or as aids to conversion. They may include funds, materials, staff, time, information or know-how.

PROCESSING

This is the manipulation or conversion of resources within the system.

CONTROLS

These are the checks, reviews, organization structures, training and other procedures which management apply to ensure that objectives are achieved.

OUTPUTS

These are the products, effects and achievements which result from processing in the system.

4.7.Audit programme

System / Process / Activity[3] ……

1	2	3	4	5	6	7	8	9
Process objectives	Control objectives	Risks	Controls	Controls evaluation	Compliance Test of controls	Substantive Test	Working Paper ref.	Conclusions Comments

Date: ……

Prepared by: ……..

Supervisor: ……..

[3] Audit program should be prepared for each system / process/ activity audited

4.8.Methods of identifying risks

In recent years there has been a considerable amount of study into the various types of risk which affect organisations and to the ways of categorising them. This section of the technical manual provides an overview of some of the main ways of identifying the risks (or threats) to achieving an objective.

The Business Risk is defined as:

> *"the threat that an event or action will adversely affect an organization's ability to achieve its business objectives and execute its strategies successfully."*

There are a number of ways of identifying the risks to an objective being achieved. Options include:

- Considering sources of risk
- Considering types or categories of risk
- Using historical experience as a manual to develop a list (i.e. know sources of problems)
- Using a control model to consider areas where risks can be created.

4.8.1.Sources of risk

The sources of risk and possible areas for the risk effect are represented in the following table:

Possible Sources of Risk	Possible Areas of Risk Effect
•commercial/legal relationships	•assets and resources
•economic	•cost: both direct and indirect
•socio-political/legal	•people
•personnel/human behaviour	•community
•financial/market	•performance of activities: how well the activity is performed
•management activities and controls	•timeliness of activities
•technology/technical	•organizational behaviour
•the activity itself/operational	•environment
•business interruptions	•intangibles
•occupational health and safety	
•property/assets	
•security	
•natural events	
•public/professional/product	
•liability	

Every source of risk can have one or several effects.

4.8.2.Types or categories of risk

Some public sector organisations consider risk under the following six categories scoring them on a scale of 1 to 5 under each relevant category. This is more precise approach when making risk assessment. The aim of scoring risks is more precisely defining the risk as low, middle or high. You should specify what do you understand under low, middle and high risk compared to assessment conditions, as explained in point 2.4. Identifying risks to this part of the Manual.

Management control environment

Score	Factor
1	High confidence in control environment; well run organization; good reputation; efficient and effective operations; sound system of internal control; recently audited with good results
2	Good confidence in control environment; audited within the last three years with reasonable results
3	Reasonable confidence in control environment; audited with significant issues within the last five years, but follow-up completed and corrective action implemented
4	Limited confidence in control environment; not audited within the last five years
5	Limited or no confidence in control environment; no prior audit coverage or fairly recent audit with significant unresolved issues or material cash losses; poor governmental reputation; high whistleblower or grievance activity

Riskiness of the nature of the work

Score	Factor
1	Low probability of loss
2	Exposure potential is relatively immaterial
3	Exposure represents a relatively low percentage of general budget operations
4	Exposure represents a relatively moderate percentage of general budget operations
5	Exposure represents a relatively significant percentage of general budget operations

Public and political sensitivity

Score	Factor
1	No press or local interest in generic topic
2	Exposure potential is relatively immaterial
3	Somewhat politically sensitive, but interest is narrowly focused to a limited audience
4	High public interest
5	Loss of funding, extreme public interest

Compliance requirements

Score	Factor
1	Few regulations; clear and simple policies, procedures and guidance
2	Limited regulations; flexibility permitted in meeting policies, procedures and regulations
3	Moderate or significant percentage of transactions subject to policies, procedures and regulations; effective and efficient business processes
4	Significant or high percentage of transactions subject to complex policies, regulations and heavy fines; unallowable cost; somewhat inefficient or ineffective processes
5	Significant or high percentage of transactions subject to complex and changing policies and regulations heavy fines; unallowable cost; somewhat inefficient or ineffective processes. High probability of monetary or funding source loss

Information and reporting

Score	Factor
1	High degree of accuracy, availability, timeliness and usefulness of information; associated information systems or applications are simple, stable or low criticality; loss of access to system generated information or reporting capability would have low budget spending unit, process or entity impact
2	Some minor issues of accuracy, timeliness or usefulness of information; Automated system with some complexity; Most reporting needs are met and any loss of access to system or reporting would have minor impact to budget spending unit process or entity
3	Some potential for information to be not timely, useful or meaningful; automated system may require some special training or expertise; system in the mid-life of implementation cycle; associated information system or application has a medium critical impacts on more than one entity, system or process
4	Uncertain reliability of data, timeliness of information or usefulness; associated information system or application are fairly complex or potentially unstable; Loss of access to system reporting will have fairly major budget spending unit processes or entity impact. Automated system may be older, with inability to provide necessary data, or newly implemented system not been fully tested; system is complex, Impacts other processes or entities or may support health & safety process
5	Low degree of information accuracy, availability, timeliness and usefulness; Information system is manual outdated or new and untested; system is highly complex, has budget spending unit wide impact, mission critical or supports life processes or activities; Computing risks have not been adequately addressed or controlled

Organizational change/growth

Score	Factor
1	Stable organization; no increase or decline in the budget
2	Limited management change or personnel turnover
3	Average turnover in key personnel, average change in prior year budget
4	Significant change in processes; downsizing; early retirements; turnover in key personnel
5	High turnover; major system changes; significant reengineering; significant change in prior year budget

4.9.Types of control

There are four basic types of control:

- ***preventive*** - designed to prevent the occurrence of inefficiencies, errors or irregularities. They cannot guarantee that inefficiencies will not occur, nor errors or irregularities, but they decrease the probability of their occurrence. Some

examples for this are the division of duties and setting up levels for approval depending of the amount to be paid.

- ***detective*** - designed to detect and correct inefficiencies, errors or irregularities. They may not give absolute assurance since they operate after an event has occurred or an output has been produced. Still, they should reduce the risk of undesirable consequences as they enable remedial action to be taken. Detective controls are most effective when they form part of a feedback loop in which their results are monitored and used to improve procedures or preventive controls. Examples include post-payment checks, stock verification and bank reconciliations.

- ***directive*** - designed to cause or encourage events necessary to the achievement of objectives. Examples include clear definition of policies and procedures, the setting of targets, and adequate training and staffing.

- ***corrective*** - to identify and evaluate alternative courses of action, to implement appropriate measures to remedy the situation and minimize damage. Examples for these controls are correcting errors during computer calculation of salaries or correcting errors when entering data in software database for the quantities of goods on stock in warehouse.

In practice the above categories may not be clearly distinguished and a single control may operate to cover two or more functions. Supervision, for example, covers three categories – detective, directive and corrective.

4.9.1.Some examples of internal controls

These examples start with the higher level controls, followed by intermediate and then low level controls. They are relevant to both manual and computer-based systems.

High level controls

Planning

This involves establishing aims, objectives and targets and the means by which they are to be achieved. Good planning includes:

- clear definitions of objectives and targets
- forecasting of activity, operational requirements and external factors which may affect the achievement of objectives
- specifying desired levels of control taking account of risk
- setting standards of performance
- defining, wherever possible, the outputs of a system and criteria for measuring them
- evaluating different options for achieving objectives
- anticipating contingencies, and devising suitable action to take in response
- indications of the relative priorities of objectives, targets and their related activities.
- budgetary constraints

Written guidance

Management's policies and procedures should be documented to ensure that all staff is aware of them and work together to achieve objectives. Written guidance and procedures manuals should be:

- clear, unambiguous and easy to refer to
- accessible to all relevant staff
- subject to checks by management to ensure that they are read and understood
- reviewed regularly, and any changes brought to the attention of staff and implemented promptly.

Organizational controls

Involves allocating responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner. Accountability and authority should be allocated to match responsibility. Major principles of good organization include:

- providing clear and documented definition of the responsibilities of individuals and groups for resources, activities, objectives and targets
- establishing clear reporting lines
- finding the most efficient balance of duties between different organizational groups
- establishing the most effective spans of command without creating more levels in the management chain than necessary
- establishing effective means of communication throughout the organization
- separating duties to avoid conflicts of interest or opportunities for abuse
- avoiding undue reliance on any one individual, particularly for internal control.

Intermediate level controls

Monitoring performance

Management needs to monitor performance to ensure that operations are conducted to achieve the optimum economy, efficiency and effectiveness. Quality control of the work should be built in to systems.

Management should establish its needs for, and use of, information about activities. Relevant information may be in the form of numbers, accounts, analyses or reports. It may be produced on a regular schedule, at management's discretion, or only when predetermined exceptional conditions are met. Management information should be reviewed regularly to ensure that it is relevant to needs and is being effectively used.

Management information should include measures and indicators of performance in respect of efficiency, effectiveness, economy and quality of service. This involves identification of inputs, including costs, and outputs and relating them to objectives.

The results of monitoring provide the basis for future action and should be linked to procedures for correcting or adjusting activities accordingly.

Evaluation

Policies and activities should be evaluated periodically for economy, efficiency and effectiveness. They should:

- be planned from the beginning of the operation
- have well-defined objectives and scope
- establish yardsticks or standards with which to make comparisons
- consider measures and indicators of performance
- identify outcomes
- identify follow-up action and provide the input for reappraisal of future options.

Staffing

Adequate staffing of management functions and operations is essential for a system to function to its full capability. Weaknesses in staffing can lead to mismanagement, error and abuse which can negate the effect of other controls. The major aspects of staffing which have control implications are:

- identifying and reviewing the staffing needs: numbers, grades, experience and expertise levels
- recruiting and selecting staff to meet the needs
- monitoring performance of individuals and groups
- arranging training and other staff development measures to achieve the full potential of staff capability.

Supervision

Supervision is the function by which managers scrutinize the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. Good supervision can raise motivation, enhance quality and assist with staff development. Poor or heavy-handed supervision can lead to de-motivated staff, which has little freedom for innovation and flexibility of response and fail to meet required standards.

Budgetary and other financial controls

The management is fully accountable for achievement of their objectives and targets. For that purpose, it is necessary to provide appropriate resources and level of expenditures. Budgetary control matches realization of objectives and achieving results with used resources and costs. Comparison between resources and costs with outputs should be applied wherever possible and e incorporated within the frames of the overall budget control system. It can be applied easily to most administrative functions, but may prove difficult in areas where costs or outputs cannot easily be quantified or where responsibilities are unclear.

Budgets should be realistic to allow for essential expenditure to achieve objectives, but should be sufficiently tight to encourage the economic and efficient use of resources.

They also should be closely linked to planning and review procedures to ensure that any proposed expenditure is essential.

Accounting controls

Organizations must keep adequate financial and other information to allow the accounts to be produced in the form prescribed. Internal auditors should understand the financial reporting requirements and the relevance of accounting standards and recommended practices. There should be adequate controls to ensure that requirements of regularity and propriety of expenditure are met.

Systems development

Controls over the development of new systems and modifications to existing systems or procedures are essential to ensure that:

- new or revised systems meet their objectives
- the effect of changes on systems and controls is properly assessed at an early stage before implementation
- systems modifications are approved and authorized
- adequate plans are made for a change from one system to another
- the implementation and application of new or revised systems and procedures are in accordance with plans.

Low level controls

Authorization

This is the approval or sanction of specified activities or transactions by a manager or other responsible person before they are undertaken. It ensures that proper responsibility is taken for the controlled activities. Key features are:

- defining the authorization requirements for activities and transactions
- allocating authority to appropriate individuals or groups
- separating responsibility for authorization from involvement in other activities which could lead to a conflict of interest
- checking that relevant activities and transactions have been properly authorized

Documentation

This involves recording information and transactions used in an organisation's business. Good standards of documentation should be established to assist and support activities and to help ensure the continuity of operations in the event of disruption. This includes the retention of information in electronic or other forms. Information must be accessible and good filing and search facilities are essential.

The work of the organization should be sufficiently well documented to enable management, external auditors or other reviewers to follow the course of operations and transactions and to identify errors, abuse or poor performance. Decisions, authorizations, transactions, checks and other information should be clearly recorded and the records safeguarded.

Standard documentation and forms can help to enforce conformity with procedures and legal requirements. They are often used to control transactions or the movement of valuables. Such documentation should be carefully designed to meet its objectives.

Completeness and accuracy

- transactions should be recorded as close to their origin as possible
- transactions should be checked at appropriate times in the processing cycle
- checks should be carried out by staff independent of those performing the activities checked.

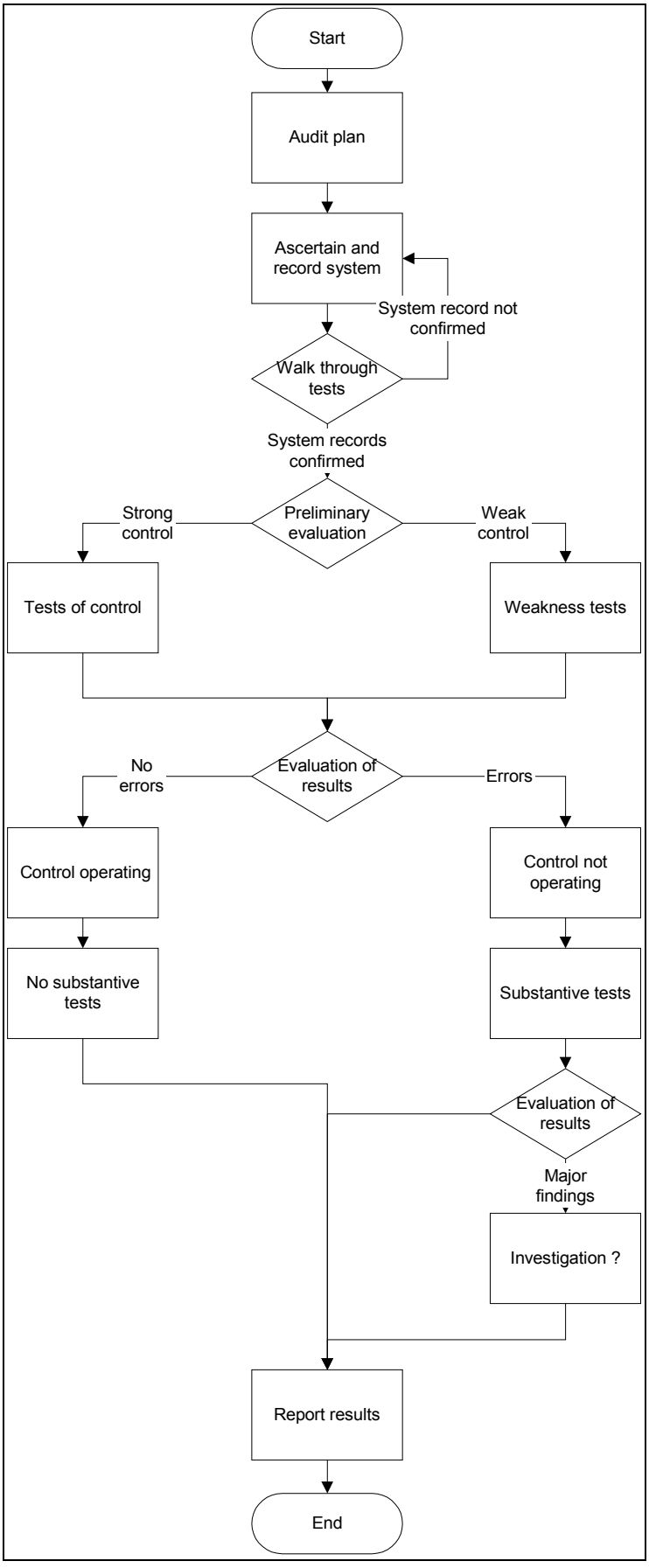
Typical controls to ensure completeness and accuracy include sequence checking, comparison with related documents, control totals, arithmetic checks, and re-performance.

Physical controls

These are concerned with the custody and safety of assets and information. They cover the whole physical environment in which systems operate. The major categories are:

- access controls (such as guards, identity cards, passwords, computer logging)
- physical checks on assets and records (such as stock takes, security inspections)
- environmental controls (such as thermostats, health and safety inspections)
- the geographical location or situation within a building of activities, and the secure custody of assets and records.

4.10.Decision points in a system based audit



1. Preparing Audit Plan
2. Evidencing and confirming of the functioning of the system through walk through test. If the evidencing of the system is confirmed, then preliminary assessment of controls is making. If you can not confirm the functioning of the system through walk through test, return back and gather additional information, until your report for the system is not identical with the system that is subject of the audit.
3. If you have an opinion that controls are strong, make control tests. If controls are weak, make tests for weaknesses.
4. Assess the test results. a) If there are no mistakes bring conclusion: controls are established well and are functioning good. There is no need of comprehensive tests. Inform about the results.
5. If you find mistakes at the functioning of controls, make comprehensive tests in order to determine the mistake and to assess the results.
6. Procure findings for main mistakes, omissions or unsuccessful controls.
7. If it is necessary, for your findings inform the head of internal audit unit, DCIA or the head of the organization with aim to assess whether it is needed further investigation.
8. Perform the audit report and stated the results.

In the text below are given additional explanations.

4.11.Planning and performing tests of control (compliance tests)

Once the objective of testing has been decided then the method of selection and sample size should be considered. Guidance on sampling is provided in **Part 3** of the Manual.

The objective of the test of control is to analyse controls and design tests which are appropriate to obtaining a reasonable degree of assurance about the operation of those controls.

The procedures required at this stage are as follows:

- record the control objective to be achieved e.g. regularity;
- record the controls in the system which purport to meet the objective;
- record the population of transactions, operations or other records to be tested;
- design tests to confirm that controls are being operated as intended.

When designing tests you should consider that the controls are analysed into different ways, thus:

- controls where there is no documentary evidence after the fact as to their execution, for instance division of duties, physical safeguarding of assets
- controls evidenced by a completed accounting routine, for instance reconciliation of control accounts, preparation of bank reconciliation, stocktaking and evaluation of stock balances
- controls evidenced by a signature, initials or by the completion of some other operation, for instance initialling boxes on a payment slip, authorising an order, matching of delivery notes and invoices and stapling them together, ticking a calculation on an invoice when it has been checked.
- controls in computer programs e.g. pricing, parameter check which can be relied on because there is good control over program development, maintenance and operations.
- supervisory controls where it is implicit that they have been carried out for instance preparing clear instructions for all operations, follow up of exception reports in management information.

4.11.1.Testing

When you are using the Test record form (**Annex 4.12.** from this part of the Rulebook) you should clearly list the transactions tested (for example invoices) in column 1 and could be located again if necessary. The tests applied are shown in the column 2 and 3. “Yes” means that the control was operated as intended, “No” means it did not and “N/A” means that the control was not applicable to that particular transaction. For every ‘No’ answer the auditor should record the reasons for this in column 4 and / or on a working paper if needed.

A “No” entry is not necessarily an error. You need to consider why the control has not been applied on this transaction.

4.11.2. Additional tests of control - rules, regulations and policies

In addition to confirming that control procedures have been operated as intended, tests of control are carried out to confirm that all internal rules, regulations and policies have been adhered to. The rule, regulation or policy should be entered in the column headed “test objective”.

4.11.3. Evaluation of test results and design weakness tests if necessary

Test results are evaluated to ensure that identified controls are being operated as intended thereby reducing the risk of errors and irregularities associated with the specific audit objective and if not, to design tests to provide evidence as to whether weaknesses have been exploited by an employee or significant errors have occurred in transaction streams.

You should analyse all the errors occurred in the testing procedure and consider the implications of the errors in relation to the effectiveness of controls. When you can obtain a reasonable explanation for an error, if this does not have continuing implications on the adequacy of an individual control, you may decide to accept the error and therefore the control. Typical examples of this are as follows:

- a delay in the performance of an accounting reconciliation - if this was caused by the responsible officer being absent on sick leave in that period and normally reconciliations were completed on time, this could be acceptable;
- an arithmetic error in a transaction - if this occurred when the person normally performing the arithmetic check was on holiday, this may restrict the auditors conclusion and further testing to that period;
- invoices issued went out with an incorrect value - if this occurred soon after the change of scales of charge and was noticed soon after and corrected this would restrict the auditors tests to the period after that time.

It can be seen from these examples that it is important for the auditor to understand the reason for the error and analyse the reason carefully because this has a significant effect on the procedures which follow. Typical possibilities after the completion of tests of control are as follows:

- the auditor finds no error - the auditor would accept that the control was operating as intended;
- the auditor finds one error - the auditor would decide whether to extend the test of control, or perform weakness tests;
- the auditor finds two errors or more which cannot be adequately explained; in this case the auditor would design weakness tests.

4.11.4. Design of weakness tests

The purpose of the weakness test is narrow down the points of system weakness and the likely sources of error. It is these potential sources of error which the auditor now sets out to explore. You need to identify:-

- the type of transaction at risk;

- specific sources of a transaction at risk from inside or outside the institution;
- specific points within the institution when the transaction is more at risk than another.

To be able to define these factors properly you need to understand the underlying reasons for the errors. To some extent these will have been highlighted when you have enquired into the causes of the errors already discovered. Furthermore when testing weakness of the control extend of tested cases (sample size, period etc) should be broaden and the focus should be on quantifying the error rate.

You should endeavour to specify tests which provide direct evidence about the extent of error for each weakness.

4.11.5.Evaluation of weakness test results

The purpose of the evaluation is to consider the evidence available about the operation of control procedures and the error rate, and decide on the further action to be taken.

At this stage the auditor should have clear evidence that:

- controls have failed because officers have not been operating controls which have been laid down by management
- there is a high error rate in the transaction stream or specific parts of it.

There are two main alternatives at this stage:

- plan an investigation (further collection of information within the legal duties and responsibilities of the IA) because errors appear to have been caused by deliberate action
- report matters to management for rectification.

In any case it may be necessary to carry out substantive tests which will assess the extent of any loss with a view to advising management to recover a loss by whatever means seems appropriate.

4.12.Test record

Test No

For examination …….. of the process……

for the period from year …….. to …….

Objective of the test:

.....

.....

.....

Examined documents / data:

.....

.....

.....

Sample selection method and sample size

.....

.....

.....

Detailed procedure

1	2	3	4	5
Checks of data or documents	**Yes**	**No**	**Comment**	**Reference**

Test Conclusion:

.....

.....

.....

Auditor ……. Date:…….

Supervisor:…….. Date:…….

4.13.Record of Audit Findings

Organisation ……. WP …….

Condition……

……

……

Standards ……

……

……

Same finding last examination: Yes …….. No …….

Procedures or practices …….

……

……

Reference to the tests ……..

Causes …….

……

……

Effect ……

……

……

Recommendation ……

……

……

Corrective action ……

……

……

Discussions: Name Title Department Date Auditor

1 ……

Comments …….

2 ……

Comments ……..

…….. ……

Auditor Date

…….. ……

Supervisor Date

4.14.Audit findings summery form

WP Ref:

Audit: ..... Financial year: .....

Prepared by: ..... Date: .....

Reviewed by: ..... Date: .....

Issues/Weaknesses	Causes	Effects	Audit File Ref	Conclusions	Recommendations

4.14.1.Fulfilling the cumulative Audit Findings Form

4.14.1.1.Issue/Weakness

This should reflect issues or weaknesses identified by audit tests. It is not necessary to provide a lot of detail - a description of one or two sentences will normally be enough.

4.14.1.2.Causes

It is important to identify the real underlying cause, and not the symptom, of each weakness. If you don't do this it is unlikely that your recommendation will result in improved control. When completing this section of the form you should ask yourself:

- ***'Why is this happening or not happening?'***

It is also worth considering

- what is the effect on performance, control, efficiency etc.?
- why do management need to know this?'

4.14.1.3.Effects

Here you should record the actual or potential impact of the weaknesses you have identified. Your audit tests will provide you with information to do this. If possible, try to quantify what the effect might be. This will allow you to make a stronger case and help to convince management of the need to implement your recommendation.

4.14.1.4.Audit file reference

Here you should record working papers which provide the detail and supporting evidence for the weakness.

4.14.1.5.Conclusion

A brief conclusion related to the weaknesses. Usually it is one or two sentences which sum up the situation. This can also be helpful when writing the audit report.

4.14.1.6.Recommendations

You should note down the main elements of your recommendations. Keep in mind the causes of the weakness and make sure that your recommendation will deal adequately with each of them.

Using this form will help you in your exit meeting with management (further guidance on handling exit meetings is given in **Part 3** in this Manual) and provide you with a good basis for discussing your conclusions and recommendations. It will also aid discussion of any alternative solutions to issues and weaknesses which may be suggested by the auditee.

4.15.Structure for audit files

4.15.1.The Permanent Audit File

SECTION	TITLE	CONTENT
1	General background information	To include: • Regulation • Strategies and plans • Organization charts • Expenditure and budgets • Volume of transactions • Other data and documents – copies or references where is the information
2	Reports to management	Copies of executive resume and action plan from all audit reports (Correspondence and other documentation to be held on relevant current audit files)
3	Copies of other relevant reports	External audit reports Consultancy reports

4	Outline of policies and procedures in operation	
5	Relevant job descriptions and authority limits	
6	Sample documentation	Any relevant forms and extracts from office instructions etc.

4.15.2.The Current Audit File

SECTION	TITLE	CONTENT
1	Audit supervision and review papers	Completed Audit Review Record and check lists
2	Audit planning documents	Audit Assignment Plan, Letter of authorisation Notes of the initial discussions with the auditee Projected and actual time budgets
3	Previous audit report	Copies of the previous Internal Audit report, including relevant correspondence and action plans
4	Points forward from previous audit	List of points highlighted for future work by Internal Audit
5	Current audit report	Draft and final versions All related correspondence Action plan Minutes of exit and final meetings
6	Follow-up to last audit	Details of tests done to check implementation of recommendations made on previous audit Summary of implemented and not implemented recommendations
7	Systems and procedures in operation	To include flowcharts, narrative descriptions and sample documentation, as appropriate
8	Form for the audit findings	
9	Audit Findings Form	Evaluation of weaknesses, causes and effects
10, 11, 12 etc.	Working papers – divided into sections (ex. by sub-system) as appropriate	To include: Headline risks Risk Identification Risk/Control evaluation Audit Test Program Audit Test Record Details of tests carried out

4.16.Audit review record

Audit:

Financial Year:

Audit stage	Auditor	CIA
Identification of (Control) Objectives		
Identification & Evaluation of Controls		
Testing of Controls		
Findings Grid		
Draft Report		

Date Report Issued: Comments:
Points carried forward to next audit: