

## **7. PLANNING THE AUDIT**

Individual audits must be properly planned to ensure:

- Appropriate and sufficient evidence is obtained to support the auditor's opinion;
- DAGP's auditing standards are complied with; and
- Only necessary work is performed.

This chapter contains guidelines that the auditor can use to plan the audit. These guidelines do *not* replace the use of professional judgment.

### **7.1 Step 1 – Establish audit objectives and scope**

It is a general principle of DAGP's audit activities that no audit entity should be subject to more than one audit in a given year. Accordingly, any individual audit may have to fulfil multiple audit objectives, so it is important that the audit is well-planned in terms of audit objectives and audit scope.

The step also involves communicating with the entity to ensure management is fully aware of the audit objectives and audit scope.

#### **7.1.1 Overall audit objectives**

Each audit will be designed to address one or more of the following objectives:

- Expressing an opinion on financial statements;
- Expressing an opinion regarding compliance with authorities;
- Testing compliance with authority or controls on selected transactions with no opinion being expressed; and
- Evaluating operational performance.

To express an opinion on financial statements the auditor needs to design audit procedures to obtain a reasonable level of assurance that the financial statements are not materially misstated. This means reaching a conclusion as to whether the account balances are valid, are complete, are properly valued, etc.

For compliance with authority work where an opinion is being expressed, the auditor will design audit procedures to obtain a reasonable level of assurance that the selected transactions in a given period are in compliance with applicable statutes and regulations. The types of irregularities that the auditor should look for will reflect the objectives of the compliance audit.

For compliance with authority audit work where there is no expression of an opinion the auditor need not plan the audit to obtain a specified minimum level of overall audit assurance.

Where the audit is to evaluate operational performance the auditor is concerned with economy, efficiency and effectiveness the auditor will develop specific audit objectives and conclude on the management framework and/or level of performance.

In summary, the nature and extent of the work that the auditor needs to perform will vary according to the objectives of the audit. Therefore, a first step in the planning process is to determine the objectives for the year.

### 7.1.2 Audit Scope

The auditor also needs to determine the overall audit scope – the total population on which to express an opinion, from which to select transactions, etc. For financial audit purpose, this total population is referred to as the “audit entity”. The audit entity determines the scope of the audit, and is generally defined by the audit mandate. For financial statement audits that are required under Section 7 of the Auditor-General Ordinance (see Chapter 2), the entity to be audited will be defined by the applicable accounting policies of the government.

For example, the accounting policies for the Federation state, “*The financial statements have been prepared by consolidating the accounts of all Centralised and Self Accounting Entities .... Commercial entities owned or controlled by the Government prepare their own financial statements, which are not included in these financial statements.*” Based on this accounting policy, the audit entity would include all centralised and self-accounting entities, but would exclude the commercial entities.

For other financial audits, the entity to be audited may need to be carefully determined. For example, a ministry may make use of a special operating agency to perform some of its functions. In this situation, the auditor will need to determine whether or not the agency falls under the scope of the audit.

In some cases, the scope of the audit can be at the auditor’s discretion, or can be negotiated with entity management. For example, DAGP may have planned to audit a particular civil works project. If the internal audit unit in that entity is planning to do a detailed audit of the project one year later, it may suggest that DAGP defer its audit by a year so the two audits could be coordinated. DAGP might decide to do so.

The first consideration in defining the scope of audit is to ensure that the work required to complete the financial attest audit is covered. In determining what else should be audited, it is important that scarce audit resources be focused on the most important aspects of the operations of the government. The first step in deciding what to examine is to identify matters of significance, both within the government as a whole and within the audit entity under examination.

Matters of significance can include one or more of the following:

- Large expenditures or large revenues;
- Areas of high risk (significant control weaknesses, potential for large losses/negative impacts);
- Matters of propriety, or probity (even if not of high materiality or risk);
- Important aspects of the programme’s performance;
- Politically sensitive areas, where the reputation of the government could be adversely affected;
- Substantial errors or misrepresentations in financial and other management reports;
- Serious problems of compliance, especially regarding laws and regulations; and

- Areas where the audit is likely to identify opportunities for significant improvement.

The auditor may decide to address one or more of these or to limit audit coverage to financial attest requirements together with the more critical aspects of compliance with key laws and regulations. Ultimately the decision as to what sub-entities are significant and should be included in a particular audit is a matter for DAGP management. As noted in Chapter 5, there are various entities that DAGP may decide to include in any specific audit. Entities may be organisational units, such as agencies, DAOs, DDOs etc., functional areas, such as the payroll function or the purchasing function, or accounting entities, such as objects of expenditure, grants or appropriations. DAGP may determine that all entities should be reviewed in a particular audit, for example ensuring complete coverage of all DDOs or grants and appropriations, and the planning phase for individual audits will be guided by this direction from management.

In determining what areas are significant, an understanding of the audit entity and its business is important. In selecting matters of significance for performance audits, the auditor should not focus only on the potential of negative findings. It is also important that key aspects of the programme are examined even if they are well managed. Providing the Legislature, the public, and also management, with assurances that programmes are well administered can be of value. When providing an assurance, the auditor must obtain sufficient evidence to conclude that there is a low risk that any significant problem has gone undetected. This usually requires much more audit effort than is required for finding weaknesses.

### **7.1.3 Entity communication letters**

DAGP has a legal mandate to perform its audit work. This mandate permits it to determine the nature, extent and timing of its work. As such, DAGP does not need to negotiate the scope of its work with the entity, or to make use of formal engagement letters.

Nevertheless, there are benefits to discussing the nature, extent and timing of the work with entity officials. These benefits include:

- The introduction of annual financial audit work has changed the nature of the audit work that the auditors are performing. Entity communication letters can be used to help the audit entities to better understand the nature of the work that is being performed, and the types of reports that may be issued at the completion of the work.
- While much of the financial audit work will be performed annually, other work that DAGP performs will continue to be performed on a rotational basis. Entity communication letters can be used to advise the entity of the nature, extent and timing of the rotational audit work that will be performed in the coming year.
- Input from entity management may help improve the planned scope of the audit and the rotational audit plan. For example, the auditors may discover that the entity's internal audit unit is planning a detailed review of the entity's internal control structure. DAGP and internal auditors could then coordinate their work, and the DAGP auditors may be able to rely on the work performed by the internal auditors.
- Input from entity management may also improve the efficiency of the audit work. For example, the auditors could advise entity officials of the planned start and completion dates of each audit, and the information that the auditors will require to perform their audit. Entity officials would then be able to locate the required information, arrange for suitable office space, etc. prior to the start of the audit.

An entity communication letter is a useful way to document the nature, extent and timing of the audit work that will be performed in the following year. A sample letter is included in the Standard Audit Working Paper Kit.

## **7.2 Step 2 – Understand the entity’s business**

### **7.2.1 Information Requirements**

Audit objectives are developed on the basis of an understanding of the entity’s business. However, the auditor does not need to have a complete understanding of all of the entity’s activities. The auditor only needs to have a detailed knowledge of those aspects of the entity’s business that relate to the audit.

For example, when performing a financial statement audit, the auditor may not need to have a detailed understanding of all of the entity’s human resource policies. However, should the auditor be performing a compliance with authority or a performance audit on the staffing and promotion processes, a more detailed understanding of the human resource policies may be required.

The auditor should assemble the following information for most audits:

- government’s plans and priorities;
- entity’s strategic plans;
- users of the entity’s services;
- legislative authorities affecting the entity’s operations;
- industry in which the entity operates, including any specialised accounting practices followed by that industry;
- activities in which the entity engages (constructing buildings, providing grants and contributions, collecting taxes, etc.);
- size of the entity (its total assets, liabilities, revenue and expenditure);
- types of transactions and documents that the entity processes;
- entity’s internal control structure; and
- economic trends that can affect the valuation of significant assets and liabilities (those held in foreign currencies, for example).

The Standard Audit Working Paper Kit includes forms to help the auditor update his/her understanding of each of these knowledge areas.

Sufficient knowledge of these matters is required by the auditor to:

- assess materiality, planned precision and audit risk;
- understand the internal control structure;
- determine components and understand how the various components and activities fit together;
- identify error conditions;
- assess inherent risk and control risk;

- understand the substance of transactions, as opposed to their form;
- identify the nature and sources of audit evidence that are available;
- update audit programmes;
- assess whether sufficient appropriate audit evidence has been obtained;
- assess the appropriateness of the accounting policies being used; and
- evaluate the presentation of financial statements and the reasonableness of the overall results.

There is a link between these knowledge areas and the tasks to be performed, as follows:

- an understanding of the users of the entity's services and the size of the entity is needed to assess materiality;
- an understanding of the legislative authorities affecting the entity's operations, the activities in which the entity engages, and the types of transactions and documents that the entity processes is needed to determine what components to audit;
- an understanding of the industry in which the entity operates, the activities in which the entity engages, the size of the entity, the types of transactions and documents that the entity processes, and economic trends are needed to assess inherent risk.

### **7.2.2 Level of Effort**

Building an understanding of the entity's business can be a significant undertaking especially where the audit scope is large, like the audit of the Federal Government. The level of effort in collecting and documenting the understanding will be high, especially when this is being done for the first time. Practically, DAGP will probably have to approach this effort incrementally over the course of the first few audit cycles. However, this should be done according to a plan that will ensure adequate depth of understanding of priority issues to provide a foundation upon which subsequent audit cycles can build.

There are a number of factors that can legitimately reduce the effort required:

- Much of the required knowledge will have already been gathered during prior compliance with authority work. This can be used when planning the audit.
- With a financial audit, the depth of knowledge required of each ministry, department etc. is relative to the materiality of that organisational unit to the overall audit scope. Therefore, the knowledge required will be small for less material agencies and will be of lower priority, so it can be deferred until more priority units have been covered.
- The depth of knowledge required also reflects the extent of intended reliance on internal controls as a source of audit assurance. If the auditor intends to place little reliance upon internal controls, then a lower level of knowledge is required than when significant reliance is to be placed on controls.

These factors can reduce the level of knowledge needed, and can render the data gathering exercise more manageable.

Once the required level of knowledge has been reached, over the course of several audit cycles, subsequent audits need only be concerned with confirming the knowledge is current and updating specific issues where necessary.

Clearly, knowledge of the business is important to all phases of the audit. The auditor should therefore be sure to update his/her knowledge of the entity's business throughout the audit. Analytical procedures are often used at the general planning phase to identify large fluctuations in the accounts from the previous year. These fluctuations, in turn, may indicate changes in the entity's operations.

Analytical procedures are discussed in more detail below.

## **7.3 Step 3 – Assess materiality, planned precision, and audit risk**

### **7.3.1 Materiality**

*Definition of materiality:* When the auditor states that the financial statements “properly present, in all material respects”, he/she is stating that the financial statements are not materially misstated. This introduces the concept of materiality.

Materiality can be defined as follows: “An error (or the sum of the errors) is material if the error (or the sum of the errors) is big enough to influence the users of the financial statements”.

Materiality is important in the context of the auditor's report on the financial statements. The opinion paragraph of a standard unqualified auditor's report commences, “In my opinion, these financial statements properly present, in all material respects, the financial position of [the entity] ...”

*Guidelines:* To determine materiality the auditor should perform the following steps:

1. Identify the probable users of the financial statements.
2. Identify the information in the financial statements that is expected to be the most important to each of these users (e.g., total expenditures, total assets or the annual surplus or deficit). One or more of these amounts may serve as the base amount(s) for computing materiality.
3. Estimate the highest percentage(s) by which the base amount(s) could be misstated without significantly affecting the decisions of the users of the financial statements.
4. Multiply the percentage(s) times the base amount(s).
5. Select the lowest amount – this is the materiality amount. Errors exceeding this value are material.

The auditor normally selects the lowest amount that results from each of these guidelines, and uses that amount for the audit of the financial statements as a whole. This is because errors often affect more than one component. For example, an error in cash may also represent an error in expenditures. As a result, the auditor cannot use a higher materiality amount to audit cash than he/she uses to audit expenditures.

Note that the materiality amount determined at this step in the general planning phase is used for the audit of *all* components. There is no need to allocate the amount to the various financial statement components. If materiality is set at Rs. 3,000,000 for the financial statements as a whole, the same Rs. 3,000,000 can be used for each financial statement component, and for each specific financial audit objective, related compliance with authority objective, and error condition.

There are some guidelines that can be used to determine the base amount(s) and the appropriate percentage(s). While guidelines should not replace the use of professional judgment, the following may be useful, depending on the nature of the entity being audited:

**Percentage of total expenditures.**

This method is the most widely used method for *not-for-profit* public sector entities. The percentages used generally range from 2% for "small" entities to 0.5% for "large" entities.

**Percentage of normalised pre-tax income.**

This method is the most used method for *profit-oriented* public sector entities (e.g., state-owned enterprises with a mandate to earn a return on their investments). The percentages used generally range from 5% for entities with "large" pre-tax incomes to 10% for entities with "small" pre-tax incomes.

**Percentage of total revenue.**

The same 2% to 0.5% range that is generally used for expenditures (see above) is often recommended.

**Percentage of equity.**

Usually 1% is suggested. This method would be appropriate only for entities following full accrual accounting and hence recording such assets as receivables, stocks and fixed assets. Without these assets, the entity would most likely be in an accumulated deficit position, and the equity amount might not be meaningful to the users.

**Percentage of assets.**

Usually 0.5% is suggested, which achieves the same materiality amount as the amount in Percentage of Equity if the debt-to-equity ratio is 1 to 1.

**Percentage of the annual surplus or deficit.**

For public sector entities, the most often quoted amount in the media is the annual surplus or deficit. It would therefore seem logical to base materiality on a percentage of the entity's annual surplus or deficit.

However, there are weaknesses in the latter approach. The main weakness with basing materiality on a percentage of the annual surplus or deficit is the fact that the amount may not represent the "true" size of the entity. An entity with an extremely small annual deficit relative to its total expenditures and revenues would have an extremely small materiality amount, and an entity with a very large annual deficit would have a very large materiality amount. In fact, basing materiality on the annual surplus or deficit could result in the materiality amount decreasing year after year even though the size of the entity being audited is increasing.

Because of these problems, a percentage of the annual surplus or deficit is normally only used as a reasonableness check on the materiality amount determined by a percentage of total expenditures or revenues.

Again, it is *not* necessary to use a percentage of total expenditures or revenue to audit the statement of expenditures and revenues, a percentage of total assets when auditing the balance sheet, etc. Instead, the auditor selects the lowest amount that results from each of these guidelines and uses that amount for the audit of the financial statements as a whole. That is because errors often affect more than one component.

Also note that available audit resources should *not* be a factor in setting materiality. Materiality is determined with the users in mind, and it is up to the auditor to ensure that sufficient audit resources are available that are required to perform the required work.

The Standard Audit Working Paper Kit contains a form that can be used to assess the materiality amount.

Ultimately, the establishment of an appropriate materiality amount is a matter for the auditor's professional judgment. For this reason, it is normally *not* appropriate to use the same materiality amount for the audit of different entities (i.e. the materiality calculated for the Federal Government as one entity, will be different from the materiality for a self-accounting commercial enterprise), and materiality should be calculated separately for each audit. In addition if, based on the knowledge of the entity and an understanding of the circumstances, the auditor believes that the monetary amount determined by the above process appears unreasonable, additional relevant factors should be considered and the materiality amount revised accordingly.

*Qualitative aspects.* In addition to the *quantitative* aspects of materiality discussed above, there is also a *qualitative* aspect. The inherent nature or a characteristic of an error may render the error material, even if its value is not. For example, a small error that is designed to conceal the over-expenditure of a government appropriation could be considered to be material by the users.

Auditors are not expected to plan financial audits to detect all of these qualitative errors. The cost of such an audit would be too high. Consequently, auditors normally ignore the qualitative aspects of errors when planning their audits. However, when reporting on the results of the audit work, they should take into account the qualitative aspects of the errors that they have found when assessing whether the financial statements taken as a whole are presented fairly.

### **7.3.2 Planned precision**

Planned precision is the auditor's planned allowance for further possible errors.

By testing a sample, the auditor can determine the Most Likely Error (MLE) in the population. However, because the auditor has only selected a sample, there is a chance that the actual error in the population is larger than that. The auditor needs to ensure there is sufficient assurance that the maximum possible error in the population is less than the materiality amount.

To do this, when planning and performing many analytical procedures and substantive tests of details, the auditor reduces the materiality amount by his/her estimate of the most likely error that will exist in the financial statements as a whole. This estimate is referred to as the "expected aggregate error." Planned precision is equal to materiality less the expected aggregate error.

To determine the expected aggregate error, the auditor should consider:

- The errors found in previous years;
- Changes the entity has made to the internal control structure to prevent these errors from recurring; and
- Other changes to the entity's business or its internal control structure that could affect the size of the errors.



If the auditor's estimate of the expected aggregate error had been set at the planning stage at Rs. 816,500, the auditor would have calculated planned precision as follows:

Materiality	Rs. 3,000,000
Expected aggregate error in financial statements	<u>816,500</u>
Planned precision	Rs. <u>2,183,500</u>

As noted in the discussion on materiality, the materiality amount determined at this step of the general planning phase is used for the audit of all components within the same audit. There is no need to allocate the amount to the various financial statement components. Consistent with this approach, the expected aggregate error being used for a particular test is the expected aggregate error in the financial statements as a whole, and *not* just the expected error in the population being audited. When auditing the completeness of income tax receipts, for example, the auditor would need to allow for errors not only in that test, but for errors found in other income tax receipts tests and for errors found in other financial statement components.

### 7.3.3 Audit risk

*Definition:* The opinion paragraph of the standard unqualified auditor's report begins "In my opinion ...". This means that the auditor is not stating that he/she is absolutely certain that the financial statements properly present the results of operations (i.e. they are not materially misstated). Rather, the auditor is stating that he/she has some degree of assurance that is less than 100% that the financial statements are not materially misstated. Generally accepted auditing standards (GAAS) refer to this degree of assurance as "reasonable assurance".

Stated another way, the auditor is taking some risk of issuing an unqualified opinion on financial statements that are materially misstated. This risk is referred to as "audit risk".

For example, if the auditor wants to be 95% confident that the financial statements are not materially misstated, this means that the auditor is prepared to take a 5% risk that he/she will fail to detect errors summing to more than the materiality amount. Audit risk is therefore 5%.

Using the audit risk and the materiality amount, when the auditor states, "In my opinion, these financial statements present fairly, in all material respects ...", the auditor is stating, "I have x% assurance that the financial statements are not misstated by more than the materiality amount".

### 7.3.4 Risk Assessment

The audit should focus on the areas of greatest materiality, significance and risk. An understanding of the risk associated with each audit entity is therefore critical to the development of an audit plan. The auditor should develop this understanding by conducting a risk assessment as part of planning an audit assignment.

In the case of a **financial attest audit**, the auditor is concerned with the risk that material misstatements exist in the financial statements that will not be detected, either by management or by audit procedures.

In the case of **compliance audits**, the auditor is concerned with the risk that certain material, or significant, transactions have occurred in a manner that contravene the laws, regulations and management procedures applying to the area of audit.

In considering audit risk, there are three categories of risk that are normally considered: Inherent Risk, Control Risk, and Detection Risk. These are discussed below.

### **1. Inherent risk**

This is the susceptibility to material/significant error or loss unrelated to any internal control system. Assessing inherent risk requires the evaluation of numerous judgmental factors, relating to the nature of the entity and its business environment taken as a whole.

This is done by asking what could go wrong and what would be the likely consequences. If the likelihood of occurrence is low and the significance of the error is low, the auditor need not be concerned. Where the likelihood is high and the significance is high, then inherent risk is high. In this situation, the auditor must be assured that either the internal controls are strong enough to detect and prevent such occurrences or the substantive audit coverage is sufficient to detect such occurrences with a high level of assurance.

### **2. Control risk**

This is the risk that material/significant error or loss is not prevented or detected on a timely basis by the internal control structure. Control risk is a function of the effectiveness of the design and operation of the internal controls. In order to assess control risk, the auditor should obtain evidence to support the effectiveness of internal control policies and procedures in preventing or detecting material error or loss. The auditor should recognise that there are risks of error or loss that cannot be detected or prevented in a timely manner whatever the controls in place. Further, the auditor should recognise that the costs of certain controls cannot be justified when compared to the potential losses they are guarding against.

The auditor should identify and evaluate both the control environment and the effectiveness of the individual internal controls that are in place. Indicators of a positive control environment include:

- policies and procedures relating to internal controls and to the need for maintaining a proper control environment exist and are documented;
- an appropriate organisational structure with clearly identified roles and responsibilities relating to the administration of internal controls exists;
- staff are selected and trained to ensure their competence and dedication in key control positions;
- senior management is involved in identifying control risks and monitoring performance;
- actions are taken to correct any identified control deficiencies with an appropriate level of priority; and
- management displays positive attitudes towards the maintenance of sound internal controls, such as: recognising dedicated effort; positively responding to audits and reviews of controls; and taking disciplinary action in response to poor performance.

The auditor is referred to the Control Environment Worksheet in the Standard Audit Working Paper Kit.

To review the effectiveness of controls the auditor should make use of the Internal Control Questionnaires which are presented in the audit programme guides as part of the Standard Audit Working Paper Kit. The auditor should expect stronger controls where risks are highest. For example, there should be strong controls in place to ensure contracts involving large

expenditures are well managed: for the selection of the contractor, for drawing up the contract; and for the control of performance under the contract. On the other hand, there should be minimal effort applied to controlling small items of inventory where the risk of loss, damage or theft is low.

The auditor should determine how the controls are applied, assess their adequacy, and identify significant control gaps.

The trend in modern government is to “let the managers manage” and take reasonable risks in order to achieve results with reduced resources. Consequently, the auditor should be conscious of the need for reasonable, but not excessive, internal controls. The cost of controls should not exceed the potential losses that could occur without those controls.

### **3. Detection risk**

This is the risk of material/significant error or loss going undetected by the auditor’s substantive audit procedures. It is a function of the effectiveness of the substantive audit procedures and audit effort.

Also, less experienced or less knowledgeable auditors are more likely to miss detecting errors than the experienced auditor. Therefore, without careful supervision, the employment of less experienced auditors increases detection risk.

**Audit risk** is a composite of these three risks. When planning an audit there is a trade off between the overall risk that the auditor will accept and the cost of the audit – the lower the overall risk that the auditor is prepared to take, the more extensive the required work and the more costly the audit becomes. Thus the risk assessment process is particularly important in determining the extent to which the audit will examine the systems, procedures, practices and transactions that govern matters at the lower end of the objective and control hierarchy.

### **7.3.5 Identification of Risk**

The auditor needs to develop the ability to identify risks. This requires an understanding of what constitutes risk and how to recognise it. There is a set of steps that the auditor can take, but experience, imagination and judgment are also critical.

The steps to follow are:

- 1 List the programme objectives, assets to be safeguarded and other results that management need to achieve;
- 2 Identify threats which could prevent achievement of these objectives;
- 3 Rate the risks, with the probability of occurrence, assuming no management controls (the inherent risks);
4. List controls and assurances which exist within the systems and practices in place (environment controls and internal controls);
5. Identify missing controls and assurances;
6. Identify risks that could occur even with the existing controls in place (control risk); and
7. Recommend improved controls and assurances (based on an assessment of the trade-off of the cost of the controls against the potential savings of lost and waste without the new controls in place).

This activity should be documented on the audit file.

### 7.3.6 Indicators of Risk

There are certain indicators that can alert the auditor to potential risk situations. Analysis of data may produce information that does not look right. Managers are often aware of high-risk situations and will assist the auditor to identify areas needing examination. This is more likely if the manager sees the auditor as an ally rather than a critic and feels comfortable confiding with the auditor.

Some examples of risk that can be encountered are:

- Processing risk;
- Programme risk;
- Regulatory risk; or
- Risk of fraud.

**Processing risk.** Errors can occur inadvertently, especially in situations such as the following:

- A new government programme where there is little experience in administering it, or the entity has taken over responsibilities for a new function and the previous administrators are no longer involved.
- New systems or procedures are introduced, especially a new computerised system.
- There have been recent changes in management or there is a high turnover of staff (in other words, there is a poor corporate memory), particularly if administrative procedures are poorly documented.
- There are unclear responsibilities.

If the process involves large transactions, the risk of inadvertent loss or waste can be serious.

**Programme risk.** Certain government programmes are particularly susceptible to significant losses, either intended (fraud) or unintended (the result of poor administration).

Examples of programmes that should be given a careful assessment of risk are:

- *Loans or guarantees*, which, by their very nature, usually place the government at risk.
- Programmes delivered by means of *contracts*, especially where there are unclear terms and conditions, insufficient specifications / performance requirements.
- *Research and development projects*, where often the results are difficult to predict (especially non-standard software development).
- Programmes with *vague outputs or outcomes*, where in return for the government's expenditures, the benefits are difficult to identify.

Large expenditures in programmes of such nature should be a high priority for the auditor to examine.

Another aspect of risk relating to programme performance is the risk that adverse publicity can arise. The danger of criticism of a programme can be out of proportion with the potential or

actual loss occurring due to some weakness in the administration of the programme. There is often a trade-off between the economic and efficient management of a programme and the cautious avoidance or mistakes that can lead to embarrassment. The auditor should be sensitive to this and be able to judge what are appropriate levels of control.

**Regulatory risk.** One means of implementing government policy is through regulatory activities. The usual purpose of regulations is to protect the public – whether this is health protection, ensuring fair trade practices, transportation safety, or other law enforcement.

Failures in a government’s regulatory programme can occur at various points within the regulatory system. For example, regulatory risk can derive from:

- inadequate laws;
- inadequate inspection/detection (insufficient resources available; untrained inspectors; poor supervision of the inspectors);
- inadequate penalties or other deterrents;
- poor records and inadequate statistics; and/or
- environmental factors outside of the regulatory process that impact on the effectiveness of the regulatory programme.

The impact of regulatory weaknesses on government operations can be significant, although not as obvious as misappropriations of funds, waste or loss of monies. For example, the non-collection of taxes can represent a huge loss to the government. Therefore the auditor must focus on regulatory activities just as much as on expenditures.

**Risk of fraud.** There are many classical indicators of weaknesses that can contribute to fraud. Some of these are:

- Insufficient separation of duties;
- Only one person with access to financial information, particularly if this person exhibits defensive or guarded behaviour;
- Weak controls;
- Inadequate management supervision, inspection, challenge or review;
- Inadequate or untimely reports; and,
- Late or non-existent reconciliations.

It is often beneficial to provide all auditors with some training in fraud awareness and investigation, and to provide extensive Forensic Audit training to one or a few auditors. Then one of those who have had extensive training and experience can be consulted wherever any serious case of fraud has been identified or is suspected.

### **7.3.7 Factors affecting audit risk**

To determine how much risk the auditor should accept that an unqualified opinion may be issued on financial statements that are materially misstated, the auditor would consider such matters as professional exposure, reporting considerations and ease of audit.

## **Professional exposure**

This is the risk of loss or injury to the auditor's reputation from litigation, adverse publicity or other events arising in connection with the financial statements reported upon.

Professional exposure risk is often considered to be highest when there is a good chance that the financial statements and the audit report thereon will undergo a lot of scrutiny. This could occur in special situations such as when an entity is:

- Receiving a lot of bad publicity for an authority violation or other matter;
- Being privatised, transferred to another level of government, or turned into a special operating agency;
- Issuing new debt; and/or
- Experiencing financial difficulty.

For audit entities such as these, the auditor may elect to reduce their audit risk to reduce their professional exposure risk.

## **Reporting considerations**

These considerations usually include the number of users and the extent to which they rely on the entity's financial statements and audit report.

## **Ease of auditing**

Factors to be considered here could include the practical availability of audit evidence and the existence of an audit trail.

### **7.3.8 Determining audit risk**

Even though the determination of audit risk is the auditor's responsibility and not the financial statement users, it may be prudent to discuss the factors affecting audit risk and the assessed level directly with the users. There are several reasons for this:

- One of the factors affecting the required level of audit risk is the extent to which the users rely on the entity's financial statements and audit report. If the users are placing extensive reliance on the financial statements, the auditor may wish to use a lower level of audit risk (i.e., obtain a higher level of overall assurance) than if the users are placing very little reliance on the financial statements. Discussing the level of audit risk with the users will provide the auditor with direct evidence with respect to this factor.
- Some of the users, such as government planners and managers as well as legislators, may be aware of special circumstances that could increase the auditor's professional exposure risk. These may include circumstances of which the auditor is not aware.

*Guidelines:* As for materiality, the assessment of audit risk is a subjective process requiring the use of professional judgment. While guidelines should not replace the use of professional judgment, the following may be useful:

<b>Situation</b>	<b>Audit Risk</b>	<b>Overall Assurance</b>
Entities perceived to be high risk (and therefore the auditor wants to achieve a high level of overall assurance and set a low level of audit risk)	3	97
All other entities	5	95

The Standard Audit Working Paper Kit contains a form that can be used to assess audit risk.

As is evident from the above guidelines, the lower the audit risk being taken, the more assurance is required. This is because audit risk and overall assurance are converses of each other. Reducing audit risk from 5% to 3% increases the desired level of overall assurance from 95% to 97%.

Increasing the overall assurance will increase the required amount of audit work. Going from 95% assurance to 97% assurance could, for example, add 20% to the total required amount of audit work.

### **7.3.9 Auditor’s responsibility to detect error and fraud**

Because the auditor designs audit procedures to detect errors in the financial statements that in total exceed the selected level of materiality, an audit most likely will not detect all immaterial errors. In fact, because the auditor is providing *reasonable* and not *absolute* assurance, there is a chance that an audit performed in accordance with GAAS will fail to detect some *material* errors. Some of these errors may be due to fraud.

Fraud is the intentional act by one or more individuals to deceive others. For example, an employee may steal cash and cover up the theft by recording fictitious expenditures. Or the employee may not record an expenditure that would cause the ministry to exceed its allowable expenditures.

The most difficult type of fraud to detect is fraud committed by management. This is because management may be able to override internal controls.

Not all frauds will result in errors in the financial statements. For example, under the accounting principles contained in the New Accounting Model (NAM), consumable stocks are not recorded in the financial statements. Therefore, the theft of inventory would not affect financial statements prepared using NAM.

When planning an audit, auditors normally start by assuming good faith on the part of management, meaning that management officials are honest and have done their best to ensure that the financial statements do not contain any errors.

However, the assumption of management’s good faith cannot be blind faith. As noted in paragraph 3.0.3 of DAGP’s auditing standards, “*The auditor should design audit steps and procedures to provide reasonable assurance of detecting errors, irregularities, and illegal acts that could have a direct and material effect on the financial statement amounts or the*

*results of regularity audits. The auditor also should be aware of the possibility of illegal acts that could have an indirect and material effect on the financial statements or results of regularity audits.”*

While the auditor is not required to actively seek out evidence of lack of good faith by management, the auditor complies with the above standard by planning and performing the audit with an attitude of professional scepticism. This means that the auditor uses a questioning mind and keeps alert for evidence that brings into question the reliability of documents or management’s representations. Should evidence come to light that indicates fraud may have occurred or the assumption of management’s good faith is not appropriate, the auditor should design specific audit procedures to deal with the matter.

Analytical procedures are a good technique to identify areas where further investigations are required. These procedures are discussed in Section 7.8 below.

Procedures to investigate possible fraud normally include a detailed review of specific projects, disbursements, etc. in which the fraud could have occurred. Sampling would normally *not* be used to detect or investigate fraud, because it involves selecting a representative sample, as opposed to zeroing in on the specific areas where further investigation is required.

## **7.4 Step 4 – Understand the entity’s internal control structure**

### **7.4.1 Definition and concepts of internal control**

INTOSAI defines the internal control structure as the plans and actions of an organisation, including management's attitude, methods, procedures, and other measures that provide reasonable assurance that the following general objectives are achieved:

- Assets are safeguarded against loss due to waste, abuse, mismanagement, errors, fraud and other irregularities;
- Laws, regulations, and management directives are complied with; and
- Reliable financial and management data are developed, maintained and fairly disclosed in timely reports.

The internal control structure of an audit entity is therefore very important to the auditor.

Furthermore, an understanding of internal controls, and the weaknesses in internal controls, is often critical for the auditor to make recommendations for improvements. If the audit focuses only on individual transactions, the auditor can only conclude, when errors are observed, that these errors should be corrected. By examining the controls over these transactions, the auditor can identify the reasons that the errors occurred. Then the auditor can recommend that the weaknesses in the controls be corrected.

Hence, it is critical that the auditor examines *controls* not just *transactions*.



## 7.4.2 General standards for an internal control structure

INTOSAI describes five general standards that entity management and employees should follow:

- *Reasonable assurance.* Internal control structures are to provide reasonable assurance that the general objectives of the entity will be accomplished.
- *Supportive attitude.* Managers and employees are to maintain and demonstrate a positive and supportive attitude toward internal controls at all times.
- *Integrity and competence.* Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to understand the importance of developing, implementing and maintaining good internal controls, and to accomplish the general objectives noted in paragraph 7.4.1.
- *Control objectives.* Specific control objectives are to be identified or developed for each activity of the organisation and are to be appropriate, comprehensive, reasonable, and integrated into the overall organisational objectives.
- *Monitoring controls.* Managers are to continually monitor their operations and take prompt, responsive action on all findings of irregular, uneconomical, inefficient, and ineffective operations.

## 7.4.3 Detailed standards for an internal control structure

In addition, INTOSAI describes six detailed standards that entity management and employees should follow:

- *Documentation.* The internal control structure and all transactions and significant events are to be clearly documented, and the documentation is to be readily available for examination.
- *Prompt and proper recording of transactions and events.* Transactions and significant events should be promptly recorded and properly classified.
- *Authorisation and execution of transactions and events.* Transactions and significant events are authorised and executed only by persons acting within the scope of their authority.
- *Separation of duties.* Key duties and responsibilities in authorising, processing, recording, and reviewing transactions and events should be separated among individuals.
- *Supervision.* Competent supervision is to be provided to ensure that internal control objectives are achieved.
- *Access to and accountability for resources and records.* Access to resources and records is to be limited to authorised individuals who are accountable for their custody or use. To ensure accountability, the resources are to be periodically compared with the recorded amounts to determine whether the two agree. The asset's vulnerability should determine the frequency of the comparison.

The extent to which these standards can be met depends to some degree on the nature of the entity. Small organisations are not always in a position to maintain comprehensive separation of duties. The auditor should take such matters into account when assessing the sufficiency of the internal control structure.

#### **7.4.4 Responsibility for maintaining internal controls**

Entity management is responsible for ensuring that a proper internal control structure is instituted, reviewed, and updated to keep it effective.

It is then the responsibility of everyone in the entity to ensure that the internal control structure functions as it should.

In addition, the Controller General of Accounts has some responsibility for maintaining an environment which promotes adequate internal control. Section 5(d) of the Controller General Ordinance states that one of the functions of the Controller General shall be “*to lay down the principles governing the internal financial control for Government departments in consultation with the Ministry of Finance and the Provincial Finance departments as the case may be*”.

#### **7.4.5 The Elements of Control**

There are five basic elements that make up a control structure:

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

*Control environment.* The control environment sets the tone for an organisation, influencing the control consciousness of the staff. It relates to:

- Management’s philosophy and operating style, including the specific way in which staff are supervised and controlled;
- The organisation structure;
- Methods of assigning authority and responsibility;
- Human resource policies and practices;
- Management’s and staff’s integrity and ethical values;
- Management’s and staff’s commitment to competence;
- Management’s reaction to change and outside influences; and
- Existence of an internal audit unit.

*Risk assessment.* Risk assessment is the identification and analysis of relevant risks to the achievement of objectives. Management needs to identify these risks in order to know the areas in which the internal control structure needs to be particularly strong. Conversely, risk assessment may indicate areas where risks are low, and therefore where the entity does not need to design elaborate internal control structures.

*Control activities.* Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the identified risks.

Control activities occur throughout the organisation, at all levels and in all functions. They include a range of activities such as:

- Proper authorisation of transactions and activities;
- Physical control over assets and records;
- Independent checks on performance; and
- Adequate segregation of duties.

*Information and communication.* Pertinent information must be identified, captured and communicated in a form that enables people to carry out their responsibilities.

To have pertinent information for accounting purposes, the entity needs to have adequate documents and records. It also needs to have prompt and proper recording of transactions and activities. This, in turn, requires a good accounting system, and a good system of communication within the organisation and with customers, suppliers, and other government entities.

*Monitoring.* Monitoring by management involves the ongoing and periodic assessment of internal control performance to determine if controls are operating as intended, and are modified when needed. Summary information should be monitored and spot checks made on the quality and timeliness of the information on selected transactions.

#### **7.4.6 The role of internal audit**

Internal audit is in itself an internal control. It acts as an independent check on performance. It can be very effective in helping management fulfil its monitoring role.

To be most effective, internal audit must *not* become part of the operational controls. The internal audit unit should not be performing checks on an ongoing basis. It should audit and review after the fact, or as a separate, independent and *additional* check, to ensure that the management and staff have been carrying out their duties properly.

#### **7.4.7 Categories of Controls**

Controls can take different forms and serve different purposes. Different ways of categorising controls are:

- Input vs. output;
- Independent vs. interrelated;
- Manual vs. electronic;
- General vs. application;
- Documented vs. undocumented;
- Preventive vs. detective; and
- Compensating.

##### ***Input vs. output***

Input controls are controls over the initial input of data. They include password controls to prevent unauthorised personnel from inputting transactions. Output controls are controls over

the output from systems. They include comparing cheques (output of payment system) to supplier invoices and other supporting documentation, and reviewing printouts of cash disbursements to ensure that all pre-numbered cheques have been recorded.

### ***Independent vs. interrelated***

A control may work on its own or may need to be part of a series of controls. For example, a reconciliation may be a powerful control in its own right, but an input control will really only be effective if the entity also has adequate controls over data processing and output.

### ***Manual vs. electronic***

Manual controls, given the fact that they are operated by staff, can be affected by human errors of judgment, misinterpretation, carelessness, fatigue, and distractions.

In contrast, electronic controls are built into computer programmes and, assuming that the systems are properly designed, installed and tested, are inherently more reliable. Any problems with the software, however, might be difficult to detect and often expensive to correct.

### ***General vs. application***

General controls are applicable to the accounting system as a whole, such as passwords restricting access to a computer network. Application controls relate specifically to a particular processing function to ensure transactions are authorised, complete and accurate.

### ***Documented vs. undocumented***

Documented controls result in evidence that the control has been performed (e.g., signatures and initials). Undocumented controls are controls where there is no evidence that the control has been performed. These would include, for example, many electronic controls where there is no evidence that the appropriate person approved the transaction. The existence of these controls can often be established through observation, inquiry and testing/replication.

Another example is when management and staff of an entity follow sound control principles based on experience. Sound controls may be in place but not documented. This presents a control exposure since the control procedures may be lost when staff turnover occurs.

### ***Preventive vs. detective***

Preventive controls prevent errors from occurring. Most data entry controls are preventive controls. In contrast, detective controls detect errors that have occurred. Most output controls and reconciliation controls are detective controls.

Preventive controls are usually less costly to use than detective controls. It is generally less costly to prevent an error than it is to detect and correct it after the fact. It is possible, however, to find systems that are so strict in preventing errors that a lot of valid data can be rejected because of minor errors or missing data elements. This can cause serious delays and expense in processing data.

### ***Compensating controls***

These are controls that detect errors that occur at earlier control points.

As a general rule, a control over output can act as a compensating control for a weak input control. For example, a control to review the list of cash disbursements to ensure that there are no missing cheque numbers can compensate for a weak control over the input of the disbursements. Similarly, if a cheque is recorded for an incorrect amount, the error will show up when the organisation performs the bank reconciliation. (This assumes that the cheque has been cleared).

#### **7.4.8 Limitations of internal control structures**

Internal control can help an entity to:

- achieve its objectives;
- comply with laws and regulations;
- ensure reliable financial reporting; and
- prevent loss of resources.

No matter how well conceived and operated, an internal control structure can only provide reasonable – not absolute – assurance to management regarding the achievement of its objectives, etc. There are limitations inherent in all internal control structures. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple errors or mistakes.

Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. In addition, the design of an internal control structure must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs.

#### **7.4.9 Multiple sub-entities and locations**

In the case of government-wide audits there will be multiple ministries, departments, etc. making up the reporting entity. Each of these may have multiple locations.

There is no requirement for the auditor to take the same approach with respect to each ministry and so on. The auditor may decide to place no reliance on the internal control structure at some Drawing and Disbursing Offices, but place a lot of reliance on some specific controls at the District Accounts Offices. In this case:

- For the DDOs, the auditor would only need an overview level understanding of controls and a general understanding of the systems to collect, record and process data and report on the results.
- For the District Accounts Offices, the auditor would need a more detailed understanding of the control environment and systems, to justify placing reliance on them.

In terms of level of effort, the auditor should already have a good understanding of the internal control structure through prior compliance with authority work. Where a given sub-entity is small compared to the materiality amount, a deep level of understanding is not required.

#### **7.4.10 Understanding and Examining Internal Controls**

The auditor is expected to review the internal controls as part of the audit.

First, the auditor should review and document the systems and procedures in place to carry out the transactions and other activities of the operations. Normally, a description of the major systems and procedures should be maintained on the permanent audit file. In which case, the auditor should review the description of the system and identify whether there have been any changes to the system.

Next, the auditor should identify points in the accounting system, and in other systems being audited, where he/she would expect to find controls.

Then the auditor should identify and document the controls at these points and determine that the controls have been operating.

Finally, the auditor should assess the adequacy of the controls and conclude whether any controls are missing or ineffective. The auditor should make recommendations to management where, in the opinion of the auditor, the controls should be strengthened. These recommendations should be based on an appreciation of the risk of reduced performance, loss, damage or waste compared to the additional costs, if any, of implementing improved controls.

A Control Environment Worksheet is provided in the Standard Audit Working Paper Kit.

#### **7.4.11 Documenting Our Understanding of Controls**

The auditor should document the internal controls as part of the audit. A clearly documented description of the controls enhances the auditor's ability to assess the controls. Also, the documentation aids supervision of the audit and improves communications between members of the team. The documentation should form part of the working papers and should be included on the permanent file.

Methods of understanding the system and application of controls include:

- Narrative;
- Flowchart;
- Internal Control Questionnaire (ICQ); and
- Walk-through.

*Narrative.* This is a written description of an entity's internal controls. Narrative of an accounting system and related controls includes four characteristics:

- Information on the origin of every document and record in the system;
- Description of all processing that takes place;
- The disposition of every document and record in the system; and

- An indication of the controls relevant to the assessment of control risk - these typically include separation of duties, authorisation and approvals and internal verification.

**Flowchart.** This is a time-consuming exercise and is generally applied only when the effort can be justified, such as when there is some uncertainty about the processes or the complexity and importance of the procedures indicate a need for clear representation.

The flowchart is a diagrammatic representation of the entity's documents and their sequential flow in the organisation and can be a valuable component of the working paper file. It includes the same four characteristics identified above for narratives.

The advantages of a flowchart are that it:

- provides a concise overview of the entity's system;
- helps identify inadequacies by showing how the system operates;
- shows clearly the separation of duties allowing the auditor to judge whether they are adequate; and
- is easier to follow a diagram than to read a description.

**Internal Control Questionnaire.** The ICQ is a common tool of the auditor. It contains a series of questions about the controls in each audit area. There is usually a pre-developed ICQ that may, or may not be tailored for the particular area under examination by the auditor. It is designed to require a "yes" or a "no" response, with a "no" response indicating potential internal control deficiencies.

The advantage of using the ICQ is it allows the auditor to thoroughly cover each audit area reasonably quickly at the beginning of the audit.

The disadvantages are:

- The individual parts of the entity's systems are examined without providing an overall view;
- A standard questionnaire may not apply to all audit entities; and
- There is a danger of taking a mechanical approach rather than thinking through the control needs of the particular operations under examination.

**Walk-Through (Cradle to Grave Test).** The walk-through is conducted to confirm that the system and controls are operating in accordance with the auditor's understanding. It is used to verify that identified controls have been put into operation.

To conduct a walk through test the auditor selects a few transactions (generally between 3 and 6), pertaining to each significant transaction cycle, and traces them through the cycle beginning with initiation of the transaction, through processing until it is ultimately summarised and included in a general ledger or management report.

The auditor should document the transactions selected for walk-through, the controls that were observed and describe any enquiries made of client personnel.

## 7.5 Step 5 – Determine components

### 7.5.1 Definition

Auditors normally do not plan audits for the financial statements as a whole. Rather, they divide the financial statements into parts and plan each part separately.

A component is a discrete item in the financial statements.

### 7.5.2 How to determine the components to be used

For a financial statement audit, the most logical way of dividing up the financial statements is to consider each line item in the financial statements to be a separate component.

“Line items” are each of the amounts reported in the financial statements, including amounts disclosed in the notes thereto.

Sometimes the financial statements include several different groupings of the same total amount. For example, expenditures may be grouped by:

- Organizational units (the ministries, departments, agencies, etc. making up the reporting entity)
- appropriation account;
- economic function (general public services, defence affairs and services, etc.); or
- object element (payroll expenditures, operating expenditures, civil works, etc.).

The auditor selects the grouping that makes it the easiest to plan, perform and evaluate the audit work. The auditor will also perform some additional procedures to ensure that the amounts reported in the other groupings are also presented fairly.

To illustrate, assume that the financial statements group expenditures by both *ministry* and by *object element*. In this case, the auditor could either plan the audit of expenditures using each ministry as a component, or using each object element as a component. If the auditor chooses “object element”, the auditor would then plan the audit to obtain reasonable assurance that payroll expenditures are not materially misstated, that operating expenditures are not materially misstated, etc. The auditor would then develop additional audit procedures to ensure that the total expenditures reported for each ministry are also not materially misstated.

For financial certification audits, it is unlikely that the financial statements will contain details with respect to expenditures, etc. by district accounts officer or by drawing and disbursing officer. However, DAGP may wish to extend the audit to include these organisational units as components to be reviewed, based on DAGP’s assessment of their risk or significance.

For compliance audits, it might be decided that individual DAOs or DDOs should be subject to review. This is at DAGP’s discretion and will be reflected in the individual audit plans.

### 7.5.3 Individually significant transactions and events

Individual significant transactions and events include:

- Very large transactions and events; and
- High risk transactions and events.



The auditor should audit 100% of these transactions and events.

Very large transactions and events are usually audited 100% because they are large enough that, should they be in error, the error could be significant. The auditor therefore does not want to risk failing to find an error in these transactions and events.

High risk transactions and events are those which, because of their nature, contain a high risk of being in error. They are often audited 100% because, while the error in each one of these transactions and events may not be significant, the high likely error rate in these transactions and events could result in a significant error in total.

Very large transactions are normally easy to find – the auditor should look for transactions and events exceeding a pre-determined amount.

High risk transactions can be more difficult to detect. The auditor should use his/her knowledge of the entity's business to identify these transactions and events.

These transactions and events are normally not treated as separate components. Rather, they are audited as part of the work performed on other components. However, there may be some cases where it is advantageous to consider them to be a separate component. This could occur when the inherent risk or control risk associated with these transactions are significantly different from the risks associated with the other transactions contained in the component.

#### **7.5.4 Using sub-components**

There may be cases where the inherent risk and control risk for part of a component are significantly different than for the rest of a component. In these cases, the auditor may decide to split the component into sub-components – the one(s) with the higher risks and the rest of the component. Higher-risk sub-components will receive a higher level of audit examination than lower risk ones.

Should the inherent risks or control risks for a particular DAO be significantly higher than for other DAOs, and if the amounts involved are substantial, the auditor should consider breaking out the single high risk office and planning its audit separately.

#### **7.5.5 Related components and transaction cycles**

Some components are related to other components. For example, an understatement of expenditures may also result in an understatement of liabilities and/or an overstatement of cash. Therefore, the audit of each of these components will provide the auditor with some assurance as to the fairness of the related components. To avoid doing more work than necessary, the auditor should take the assurance achieved from auditing the related components into account.

One way to do this is to consider transaction cycles – the flow of the transactions. For example, the purchase of a medical supply will result in a stock item that will either be in expenses for the year or in the year-end stock balance. The purchase will also result in a cash disbursement or a payable at year end.

The internal control questionnaire and audit programmes contained in the Standard Audit Working Paper Kit and Audit Guides contain the “standard” components for the entities being

covered, and use a transaction cycle approach for the tests of internal control. It must be stressed that the auditor needs to assess inherent risk and control risk for each component and specific financial audit or compliance with authority objective, as opposed to each transaction cycle and specific financial/compliance audit objective.

## **7.6 Step 6 – Determine financial audit and compliance with authority objectives, and error/irregularity conditions**

### **7.6.1 Specific financial audit objectives**

Having divided the audit into components, the next step is to define what we mean by “properly presents” in the audit certificate. To do so, the auditor needs to consider what he/she would consider to be an error.

For a financial statement audit, a component is considered to be in error if:

- it is not valid (the asset or liability does not exist or the revenue or expenditure has not occurred);
- the asset, liability, revenue or expenditure is not complete;
- the transactions have not been carried out in proper compliance with relevant laws, regulations and administrative rules;
- the asset or liability is not properly valued or is misclassified, or the revenue or expenditure is not properly measured or is misclassified; or
- the financial statement presentation is not proper.

The Standard Audit Working Paper Kit and Audit Guides make use of these specific financial audit objectives.

To illustrate, payroll expenditures may be materially misstated if:

- the costs are not valid. This could be due to, among other things, ghost workers on the payroll.
- the costs are not complete. For example, employees have not been paid, or the payments have not been recorded.
- the costs are not properly measured. This could be due to paying employees more or less than they should be paid, or the amounts being recorded being more or less than the actual payments.
- the financial statement presentation is not proper. This could be due to the failure to disclose all of the information called for in the New Accounting Model.

### **7.6.2 Related compliance with authority objectives**

Reviewing compliance with laws and regulations is very important. Decision makers need to know if the laws and regulations are being followed, whether they are having the desired results and, if not, what revisions are necessary.

Section 3.4 of DAGP’s auditing standards states, *“In conducting [financial] audits, a test should be made of compliance with applicable laws and regulations.”*

To comply with this standard, the auditor need not test for compliance with *all* laws, regulations, rules, policies, etc. As noted in paragraph 3.4.3 of DAGP’s auditing standards, *“Because the laws and regulations that may apply to a specific audit are often numerous, the auditors need to exercise professional judgement in determining those laws and regulations that might have a significant impact on the audit objectives.”*

For financial audits, Section 3.4 of DAGP’s auditing standards requires the auditor to *“design audit steps and procedures to detect errors, irregularities, and illegal acts that could have a direct and material effect on the financial statement amounts or the results of regularity audits. The auditor also should be aware of the possibility of illegal acts that could have an indirect and material effect on the financial statements or results of regularity audits.”*

In deciding which laws and regulations should be examined as part of a financial audit, the auditor should deal with those laws and regulations that might have a significant impact on the financial audit objectives.

In addition to compliance audit work performed as part of a financial audit, DAGP also conducts extensive compliance tests to identify deviations and validate controls at organisational units across the Government of Pakistan.

Departments, ministries, etc. are not permitted to spend, borrow or raise revenue without the approval of Parliament. Therefore, audits of compliance with authority should focus on compliance with authority to spend, borrow and raise revenue, as follows:

### **Spend**

Determine that:

- the services were actually performed or the goods were actually received;
- the expenditure is consistent with the nature of the appropriation to which it was charged;
- the expenditure does not result in the total approved expenditure being exceeded; and,
- the expenditure is in accordance with the applicable legislation and the rules and regulations issued by such legislation have been complied with.

### **Borrow**

- Determine that the amount and debt terms (period, interest rates, repayment schedule, etc.) are in accordance with the appropriate law.

### **Raise revenue**

Determine that the cash received is:

- for an approved tax or other approved revenue source; and,
- is received in accordance with the applicable legislation and the rules and regulations issued by such legislation have been complied with.

The compliance with the authorities tests noted above apply to organisational, functional or accounting units for different types of government body as follows:

*Federal and provincial governments.* All the authorities described in the preceding section would usually be considered part of the audit of federal and provincial governments.

*District governments.* District governments are not permitted to borrow. Therefore only authorities to spend and to raise revenues would normally be considered part of the audit of a district.

*State-owned enterprises.* These enterprises are usually created by separate acts. These acts and the supporting regulations usually specify the operations that the enterprise is permitted to carry out. Compliance with the spending, borrowing and revenue-raising authorities in these acts and regulations is therefore usually the principal focus of the compliance with authority work for these audits.

### **7.6.3 Potential Error conditions**

The last part to this step is to consider error conditions. The idea here is to consider ways in which an asset, liability, revenue or expenditure item might not be valid, might not be complete, etc. Put another way, the auditor's objective is to identify ways in which a monetary error can occur in the financial statements, or an applicable authority may not be complied with.

There are probably numerous reasons why a component might not be valid, might not be complete, etc. However the chance of some of them occurring might be negligible. Similarly, the maximum possible error that could result from some of them might be insignificant. The auditor's objective is to identify the errors that have a real chance of occurring, and that could be relatively large in relation to the materiality amount. For this reason, error conditions are sometimes referred to as "potentially big errors".

Note that conditions that constitute an error will be affected by the accounting policies being used. For example, if the accounting policies do not call for the recording of accounts payable, then the failure to record a payable would not constitute an error. However, there should be a system to track unsettled payables in the form of commitments against appropriations.

The process of determining which error conditions or compliance deviations should be audited will help to ensure that the audit plan is complete. The process will also help to ensure that the audit plan does not include unnecessary work. The process therefore helps to ensure that auditors spend their time dealing with matters of real importance, and do not waste their time on insignificant matters.

For example, consider the component "payroll expenditures".

For the *completeness of payroll expenditures*, the auditor considers how payroll expenditure figures might not be complete and may identify the following three error conditions:

- Services performed have not been paid for;
- Payments made have not been recorded in the payroll register; and
- The amounts in the payroll register have not been included in the financial statement amounts.

In addition, the auditor needs to consider whether there are any related compliance with authority objectives. In this case, because compliance objectives relate to controlling what has been spent, as opposed to ensuring that the spending is complete, there are no related compliance objectives.

Consider the *validity* and *measurement* objectives for *payroll expenditure*. The auditor may identify four additional error conditions, as follows:

- Services paid for were not performed (because, for example, there are ghost workers on the payroll);
- Employees have been paid more or less than they should be paid;
- Payroll expenditures are recorded in the Payroll Register at the wrong amount;
- Payroll expenditures have been charged to an incorrect account or appropriation; and
- Amounts in the payroll register have not been included in the financial statements at the correct amount.

In this case, the auditor may also identify the following *compliance with authority* matters:

- The work being performed was not properly approved;
- Pay rates/employee levels were not properly approved in accordance with regulations; and
- The payments were not properly approved.

The same approach can be applied to receipts. For example, for the *completeness of income tax receipts*, the auditor may identify three error conditions, as follows:

- Income tax receipts are not deposited in the bank;
- Income tax receipts are not recorded in the cash receipts register; and
- The amounts in the cash receipts register are not included in the financial statement amounts.

In addition, the auditor needs to consider whether there are any related *compliance with authority objectives*. In this case, there probably is one – that the receipts were deposited within the time period required by government policy.

For the *validity* and *measurement* objectives for *income tax receipts*, the auditor may identify two other error conditions, as follows:

- The income tax receipts are being charged to an incorrect account; and
- The amounts in the cash receipts register are not included in the financial statements at the correct amount.

In addition, the auditor may also identify one *compliance with authority* matter – the government did not remit any overpayments by the taxpayer back to the taxpayer on a timely basis.

#### **7.6.4 How error conditions and compliance irregularities are used to develop audit programmes**

The error conditions/compliance deviations provide the auditor with guidance as to which audit procedures should be included in the audit programme. Using the errors/irregularities identified above, for regularity and measurement of payroll expenditures for example, the auditor can develop audit procedures to determine if:

- Services paid for were actually performed;
- Employees were paid correct amounts;
- Payments are being recorded in the payroll register at the correct amount
- Payments are recorded in the correct account and appropriation at the correct amount;
- Amounts in the payroll register are included in the financial statements at the correct amount;
- The work performed was properly approved;
- Payments made were properly approved.

Similarly for the regularity and measurement of income tax receipts the auditor could develop procedures to determine if:

- Receipts are posted to the correct account;
- Amounts in cash receipts register are included in the financial statements at the correct amount;
- Government is remitting overpayments back to taxpayers on a timely basis.

### **7.7 Step 7 – Assess inherent risk and control risk**

Inherent risk and control risk may differ by component and audit/compliance objective. As a result, the auditor may have a large number of different inherent and control risk valuations to deal with.

It is tempting to combine different risks by using a weighted approach. However, this approach is not recommended as it fails to meet the standards for generally accepted auditing standards.

#### **7.7.1 Inherent risk**

Inherent risk is the chance of material error occurring assuming that there are no internal controls in place. “Material error” may be one error or the sum of multiple smaller errors.

Inherent risk is evaluated at this stage to determine how much testing of internal controls and substantive testing (analytical procedures and substantive tests of details) the auditor needs to perform to achieve the desired level of assurance. In general, the greater the inherent risk, the greater the audit effort required.

Inherent risk is assessed assuming that there are no internal controls in place. As such, it is assessed in a hypothetical environment.

Factors affecting inherent risk include:

*The nature of the component.* Components such as cash are more susceptible to manipulation or loss than, say, fixed assets.

*The extent to which the items making up the component are similar in size and composition.* If the population is composed of relatively homogeneous items, it would be easier for management (and the auditor) to detect anomalous transactions and amounts.

*The volume of activity.* If there are a lot of transactions being processed, the chances of an error occurring may be higher than if only a few transactions are being processed.

*Competence of the staff processing the transactions.* If staff are experienced and take their jobs seriously, there is probably a lower inherent risk than if they are inexperienced or careless.

*The number of locations.* Entities operating out of a single location with a centralised accounting system may have a lower inherent risk than those operating out of many locations, each with its own accounting system.

*The accounting policies being used.* Many components have a lower risk of error when the cash basis of accounting is being used than when the accrual basis of accounting is being used.

*Factors that could affect the risk of fraud.* An error could be an intentional one. The auditor should use a questioning mind and be alert for evidence that contradicts or brings into question the reliability of documents or management's representations.

It can be seen from the above that evaluation of inherent risk is based primarily on the auditor's knowledge of the entity and its environment. This knowledge would have been acquired primarily in Step 2 of the process – updating the understanding of the entity's business.

The assessment of inherent risk will be subjective, and will require the use of professional judgment. It would therefore be appropriate to have the most experienced and knowledgeable individuals on the audit team make the assessment of inherent risk. These should be the individuals with the greatest knowledge of the entity being audited.

Inherent risk may differ by component and by specific financial audit objective. For example, the risk of cash being improperly valued is low, but the risk of cash not being complete may be quite high.

Inherent risk needs to be assessed throughout the audit. For example, if inherent risk is assessed as "low" at the general planning phase but numerous errors are found during the fieldwork phase, then the assessment of inherent risk may need to be revised.

While guidelines should not replace the use of professional judgment, the following may be useful when assessing inherent risk:

<b>Level of Inherent Risk</b>	<b>Risk</b>	<b>Resulting Assurance</b>
High inherent risk	60%	40%
Moderate inherent risk	50%	50%
Low inherent risk	40%	60%

Risk assessment is a matter for DAGP and will reflect ground realities within the entity being audited. It is recommended that a conservative approach be considered until DAGP gains experience with this methodology, to recognise the danger of using an incorrectly low risk factor. Assume the auditor sets inherent risk at a low 20%. At this level, the auditor could eliminate all or most substantive sampling, and little work would be required on the component. Given this low level of planned effort, if there are significant monetary errors or compliance irregularities they are likely not to be detected, and in the worst case, the auditor might issue an unqualified report when there were actually material errors present.

Accordingly, an inherent risk factor of not less than 40% is recommended unless there is convincing evidence such as prior compliance with authority audit work that detected a high level of compliance or few monetary errors.

The Standard Audit Working Paper Kit includes an Inherent Risk Assessment Form that can be used to assess inherent risk.

### **7.7.2 Control risk**

Control risk is the chance that the entity's internal controls will not prevent or detect material error and is directly related to the effectiveness of the internal control structure.

Control risk is evaluated at this stage as it establishes a limit on the amount of assurance that the auditor can obtain from tests of internal control.

Much of the work required to assess control risk would have been performed as part of updating the understanding of the entity's internal control structure.

Control risk is also affected by the factors that could affect the risk of fraud – particularly management fraud. This is because management can often override the internal controls that have been put in place. As discussed above, the auditor needs to use a questioning mind and stay alert for evidence that contradicts or brings into question the reliability of documents or management's representations.

Control risk may differ by component and by specific audit objective and related compliance with authority objective. For example, entity management may have devised very good controls over the payment process to ensure the validity and measurement of expenditures, but may have paid less attention to the completeness of those expenditures.



In general, the control environment and the controls that collect, record, process and report often have a pervasive effect on many components, financial audit objectives and related compliance with authority objectives. The controls that enhance reliability are the ones that are most likely to differ by component and by specific audit objective.

Control risk needs to be assessed throughout the audit. For example, if control risk is assessed as “low” at the general planning phase but numerous internal control deviations (improperly approved supplier invoices, for example) are found during the fieldwork phase, then the assessment of control risk may need to be revised.

While guidelines should not replace the use of professional judgment, the following may be useful when assessing control risk:

<b>Level of Control Risk</b>	<b>Risk</b>	<b>Resulting Assurance</b>
High (poor internal controls)	80%	Up to 20%
Moderate (moderate internal controls)	50%	Up to 50%
Low (strong internal controls)	20%	Up to 80%

The reason for presenting “Resulting Assurance” as an amount “up to” a percentage limit is that, unlike inherent assurance, control assurance must be earned. The auditor should not rely on the internal controls unless tests demonstrate that the controls are not only in place, but are also working.

To illustrate, the auditor may have concluded that the internal controls over the validity and measurement of payroll expenditures were moderate. The auditor may therefore have assessed control risk as “moderate” (50%). This means that, for this component and these specific financial audit objectives, the auditor can place moderate reliance (50%) on the internal control structure.

To place moderate reliance on the internal controls the auditor must do a fair amount of testing of internal controls. The auditor may decide that it is more efficient to place only limited reliance on the internal control structure and instead do extensive analytical procedures and use a large sample for substantive tests. In this case, even though the auditor may have been able to obtain a control assurance of 50%, the auditor may decide to do only enough tests of internal control to support a 20% level of assurance. The auditor would then set control risk at 80%.

It has been noted that control risk is assessed at this stage as it limits the amount of assurance the auditor can obtain from his/her tests of internal control. Assume that, in the above illustration, the auditor wants to place a lot of reliance on the internal control structure. Because control risk was assessed at 50%, it is not possible for the auditor to obtain more than a moderate level of assurance from the internal controls.

Put more simply, it is not possible to place a lot of reliance on a poor internal control structure.

To provide some practical guidance, consider the following questions:

**Question 1:**

Should the control environment in all DDOs be documented, or should only the controlling offices be taken into account?

Answer:

This answer refers back to a basic auditing concept – the auditor should document and test any controls on which reliance is to be placed. Therefore, any controls, in any DDOs, on which the auditor intends to rely should be documented.

**Question 2:**

If the controls in one department are not reliable, should it affect the auditors view of the overall control environment?

Answer:

If the controls in one department are not reliable, but in other departments they are, the auditor can assess control risk as “high” where they are not reliable, and “low” in the other departments. The auditor should not attempt to come up with an “average” risk assessment.

**Question 3:**

What would be the relative weightings of authorisation and accounting controls? That is to say, how would the auditor’s assessment be affected if the authorisation controls are working and the accounting controls fail more often than not?

Answer:

As for the response to Question 2, the auditor should not attempt to derive an aggregate risk assessment. In this case, the auditor may decide to rely on the authorisation controls, but cannot rely on the accounting controls.

Since the auditor would need to take a substantive approach with respect to transactions flowing through the system because of the poor accounting controls, relying on the authorisation controls would not likely reduce the amount of the required substantive testing. Therefore, the most cost effective approach would likely be to assess control risk for the particular transaction cycle as high and audit accordingly.

**Question 4:**

What aggregation and consolidation mechanism should be used to develop an overall assessment of the control environment prevailing in the Federal Government.

Answer:

Because the Federal Government is made up of many sub-entities, each of which has its own risk profile, it is not appropriate to try to derive an aggregate risk assessment. Separate control risk assessments are made for each financial audit and compliance with authority audit objective for each component, within each sub-entity.

**Question 5:**

Suppose in all but two of the sub-offices of a ministry, controls can be relied on, but they cannot be relied upon for the remaining two sub-offices. Suppose also that the control environment in the DDOs is poor. How should the auditor proceed?

Answer:

The auditor could assess control risk as “low” in all but the two sub-offices and plan to rely on the related controls, while not relying on controls in the “high” risk sub-offices. Since the control environment in the DDOs is poor, the auditor may be forced to a substantive approach with respect to the transactions flowing through the system. Relying on the controls in the sub-offices may therefore not reduce the amount of required substantive testing. If that is the case, the most cost effective approach would probably be to assess control risk for the particular transaction cycle as high.

**Question 6:**

If the auditor does not aggregate the risk assessments of individual sub-entities, components and objectives, won't the auditor end up with hundreds of different assessments of control risk? And won't it take an auditor considerable time to come up with all those different assessments?

Answer:

Theoretically, it is possible that the auditor will end up with hundreds of different assessments of control risk. However, in practice this is not generally the case and the auditor often winds up taking approximately the same approach for many different components, specific financial audit objectives and related compliance with authority objectives. There are several reasons for this:

The control environment often applies quite widely across components in each sub-entity. As a result, if it is possible to place a lot of reliance on the internal controls for one component, it is normally possible to place a lot of reliance on internal controls for many of the other components in the same sub-entity.

Also, as noted previously, components may be inter-related. For example, an understatement of cost of sales may also result in an overstatement of the year-end stock balance and/or an understatement of the year-end accounts payable balance and/or an overstatement of cash. One particular audit procedure, such as testing the validity and measurement of cost of sales, may also provide assurance as to the validity and valuation of the year-end stock and accounts payable balances. It therefore often makes sense to use approximately the same sources of assurance for these related components.

Regarding the amount of time required to perform multiple assessments, it is true that the level of effort will be greatest when first assessing each control risk. Once the various controls have been assessed, the auditor would only need to consider the impact of changes in the nature of the entity, the results of the previous year's audit, and so on, as opposed to repeating the entire exercise from scratch.

Recognising the challenge of establishing initial risk assessments across large audit entities, it is suggested that DAGP consider a phased approach to risk assessments, and accepts that audits for the initial years will not cover all aspects of risk assessment because of resource and time constraints. This is not intended to provide a justification for weak execution of audit procedures, but recognises that it may take a number of audit cycles for rigorous audit procedures to be applied across all aspects of each audit. It is suggested that DAGP strategic audit plans for the first few years of implementing these new audit procedures should accommodate this phased approach.

The Standard Audit Working Paper Kit contains a Control Risk Assessment Form that can be used to assess control risk.

## **7.8 Step 8 – Determine mix of tests of internal controls, analytical procedures and substantive tests of details**

### **7.8.1 Introduction**

Financial audit procedures are usually broken down between tests of internal control and substantive tests supplemented with compliance with authority tests. DAGP also conducts audit activities which focus exclusively on compliance with authority testing.

Tests of internal control are used to gain assurance that specific controls within the entity's internal control structure are operating effectively, and are therefore helping to reduce the chance of material error existing in the accounting information.

Substantive tests are procedures used to gain direct assurance as to the completeness and accuracy of the data produced by the accounting systems. They are often broken down between analytical procedures and substantive tests of details.

Audit procedures that provide both assurance with respect to internal controls and substantive assurance are often referred to as "dual purpose" tests.

Compliance with authority procedures are used to determine whether entity staff have fulfilled the administrative requirements of all applicable rules, regulations and legislation.

### **7.8.2 Tests of internal control**

Tests of internal control include:

- Inquiries of appropriate entity personnel;
- Observation of policies and procedures in use;
- Walk-through procedures; and
- Selecting a sample of transactions and verifying that the appropriate control procedures were followed.

The first three procedures are the same as were used to update the understanding of the internal control structure. The work done at that stage will have already provided some assurance with respect to the internal control structure.

With respect to sampling, if the auditor wishes to place high reliance on a specific internal control, it is normally necessary to test the control throughout the entire year. If, on the other

hand, the auditor only wishes to place moderate reliance on the control, it may be sufficient to select a sample of transactions to an interim date (say, the first 8 months of the year), and then to use inquiries, observations and walk-through procedures to ensure that there have been no changes made to the internal control structure between the interim date and the year-end date.

If the auditor only wishes to obtain limited reliance on a particular internal control, then sampling is often not required at all –inquiries, observations and walk-through procedures may provide all of the required assurance.

GAAS do not permit the auditor to obtain all of his/her assurance through tests of internal control – some substantive testing must always be performed. This is because the ability of the internal control structure to prevent or detect material error is subject to practical limitations, such as:

- Members of management may be in a position to override specific internal controls.
- Collusion can circumvent internal controls that depend on good segregation of duties to be effective.
- Inexperienced entity officials may not perform their control procedures properly. There is always a possibility of human error.
- Internal controls are often designed to address transactions arising from the normal course of the entity’s activities. They may not cover transactions of an unusual nature, or arising from new activities.
- Management may not be prepared to devote the resources that would be required to prevent or detect all errors. Rather, management normally requires that the internal controls be cost-effective. This means that the benefits of having the controls must exceed their costs.

### **7.8.3 Analytical procedures**

Analytical procedures are techniques used by the auditor to:

- Form expectations as to what the recorded amounts should be by studying the relationships among elements of financial and non-financial information;
- Compare those expectations with the recorded amounts; and,
- Draw conclusions about entity operations, inherent risk and control risk, and the completeness and accuracy of the recorded amount.

Analytical procedures are an efficient and effective way to obtain audit assurance. As a result, they should be performed on every audit.

Analytical procedures may be used in all phases of the audit to achieve various objectives, for example:

Planning phase:

- To obtain knowledge of the entity’s business operations;
- To identify unusual items and explore areas of potential high inherent risk; and
- To obtain some degree of audit assurance.

Fieldwork phase:

- To obtain the planned degree of audit assurance.

Evaluation phase:

- To assess the internal consistency and overall reasonableness of the financial statements using the auditor's knowledge of the entity; and
- To obtain some degree of audit assurance.

The auditor can derive various levels of assurance from analytical procedures depending on how rigorously the analytical procedures are designed and performed.

There are several different types of analytical procedures, as follows:

#### **General reviews for reasonableness.**

These analytical procedures involve a high level comparison of current information with previous periods, budgets or statistics from the entity. No pre-determined threshold amount is specified for identifying significant fluctuations. The process is sometimes referred to as “eyeballing” the financial statements – looking for accounts that appear to be unusual in amount, in volume of activity, etc. The objective of this type of analysis is generally to decide where to focus audit attention.

#### **Comparative analysis.**

This involves comparing the current year's reported amounts (or ratios) with those of the prior years. Comparative analysis assumes that the prior year's amount is a sufficiently accurate estimate of the current year's amount and, therefore, can be used to identify any significant fluctuations from the current year's recorded amount. A pre-determined threshold amount is specified for identifying significant fluctuations.

#### **Predictive analysis.**

Predictive analysis compares the current year's reported amounts (or ratios) with a prediction of what the current year's amount (or ratio) should be, based upon the trend of the prior years' amounts (or ratios). The prior years' data used in making the prediction is adjusted for all known changes in the factors affecting the data. This usually results in a more precise estimate than comparative analysis. A pre-determined threshold amount is specified for identifying significant fluctuations.

#### **Statistical analysis.**

This category of analytical procedures involves analysing the known behaviour of variables and developing an equation (model) that explains the relationship between these variables. Although this category is similar to "predictive analysis", the distinguishing characteristics of statistical analysis is that it uses more rigorous methods, such as regression analysis, to provide more accurate predictions and objectively measures the confidence level and the achieved level of precision.

#### **Overall verification procedures.**

This category of analytical procedures involves building up an estimate of an account balance from known and verified data. For example, the auditor could verify the number of rental units by type of unit, the average rent by type of unit, and the vacancy rate. The auditor could then compare the product to the revenue received from the rents. Overall verification procedures usually result in an accurate estimate of the account. A pre-determined threshold amount is specified for identifying significant fluctuations for the auditor to investigate.

Care is required with this type of analysis. The auditor must not assume that the data are more accurate than the financial information. For example, the actual vacancy rate may be lower than the recorded vacancy rate, with the difference being due to fraud. Thus the analytical

data might substantiate the financial data, while income being received is less than income due. The auditor should therefore test whether sources of information are independent or might be subject to the same potential errors.

Appendix B discusses each of these types of analytical procedures in detail. The discussion includes a description of how the auditor normally determines the pre-determined threshold amount.

The following table provides guidance as to the amount of assurance that each category of analytical procedure can provide. While guidelines should not replace the use of professional judgment, the following is typical:

<b>Type of Analytical Procedure</b>	<b>Risk</b>	<b>Assurance</b>
Overall reviews for reasonableness	100%	0%
Comparative analysis	70% or more	Up to 30%
Predictive analysis	50% or more	Up to 50%
Statistical analysis	30% or more	Up to 70%
Overall verification procedures	10% or more	Up to 90%

The Standard Audit Working Paper Kit contains an Analytical Procedures Assessment Form that can be used to assess the amount of assurance that the auditor can derive from the different categories of analytical procedures.

Appendix B also discusses the fact that computer-assisted auditing techniques (CAATs) are a very useful tool for performing analytical procedures. With the use of a CAAT, the auditor can perform numerous analyses instantaneously. If performed manually, the equivalent work could consume extensive audit effort.

CAATs are discussed in more detail in Appendix C.

#### **7.8.4 Substantive tests of details**

Substantive tests of details include such procedures as physically inspecting an asset, checking transactions recorded in the books and records to supporting documentation, and confirming amounts with third parties.

The auditor usually tests a sample of transactions as opposed to verifying 100% of them.

Appendix B contains a detailed description of sampling.

Substantive tests of details can involve more than sampling. There are often specific transactions and events that the auditor wants to examine. These could be:

- Very large transactions and events; or
- High risk transactions and events.

These transactions and events are often referred to as “individually significant transactions and events”. They are often audited 100% because they are large enough that, should they be in error, the error could be significant. The auditor therefore does not want to risk failing to find an error in these transactions or events.

Auditors often audit 100% of the individually significant transactions and events, and audit a sample of the remaining transactions.

### **7.8.5 Compliance with authority tests**

The first step for the auditor is to work with entity management to identify the rules and regulations that apply to the entity. Of these, the auditor will determine which authorities are most significant and will design tests to check compliance. The auditor will also determine what sampling approach is appropriate. Sampling is discussed at length in Appendix B.

The auditor will then plan to extract the samples as determined, and apply the compliance tests.

### **7.8.6 The audit risk model**

The audit risk model is a useful way to tie together all of the various sources of audit assurance.

The basic theory behind the audit risk model is that, for errors adding up to more than materiality to remain in the accounts at the end of the audit (audit risk - AR), all of the following must have happened:

- The errors must have occurred in first place (inherent risk - IR);
- The internal controls must have failed to prevent or detect the errors (control risk - CR); and
- The auditor’s substantive procedures (analytical procedures and substantive tests of details) must have failed to detect the errors (detection risk - DR).

Basic probability theory states that, if two events are mutually exclusive (the occurrence of one is not affected by the occurrence or non-occurrence of the other), then the probability of both events occurring is the probability of the first event occurring times the probability of the second event occurring.

All of the events in paragraph, as defined, are mutually exclusive, and all must occur before errors adding up to more than materiality remain in the accounts at the end of the audit. We therefore have the following formula:

$$\begin{aligned} \text{AR} &= \text{IR} \times \text{CR} \times \text{DR}; \text{ where:} \\ \text{AR} &= \text{Audit risk;} \\ \text{IR} &= \text{Inherent risk;} \\ \text{CR} &= \text{Control risk (achieved); and} \\ \text{DR} &= \text{Detection risk.} \end{aligned}$$

The reason for qualifying the control risk as being “achieved” is because the auditor needs to validate his/her control assurance. What goes in the risk model is the converse of the achieved assurance.



The audit risk model is often expanded upon to split detection risk (DR) into two parts. This is done for two reasons:

1. Analytical procedures are often effective and efficient at obtaining audit assurance. As a result, they should normally be performed on every audit. The assurance to be achieved from these procedures needs to be reflected in the risk model;
2. The auditor often performs more than one substantive test of detail to obtain the required assurance with respect to each specific financial audit objective and related compliance with authority objective. To link the risk model to the confidence level to be used for one key substantive test of details, these other substantive tests of details need to be considered separately.

It is done as follows:

$$\begin{aligned}
 AR &= IR \times CR \times DR \\
 &= IR \times CR \times OSPR \times STDR; \text{ where:} \\
 AR &= \text{Audit risk;} \\
 IR &= \text{Inherent risk;} \\
 CR &= \text{Control risk (achieved);} \\
 OSPR &= \text{Other substantive procedures risk, being the} \\
 &\quad \text{risk that the auditor's analytical procedures,} \\
 &\quad \text{and all substantive tests of details expect one} \\
 &\quad \text{key substantive test of details, will fail to detect} \\
 &\quad \text{material error; and} \\
 STDR &= \text{Substantive test of details risk, being the risk} \\
 &\quad \text{that one key substantive test of details will fail} \\
 &\quad \text{to detect material error.}
 \end{aligned}$$

The reason for splitting out one key substantive test of details in this manner is that the formula can be rearranged as follows:

$$STDR = \frac{AR}{IR \times CR \times OSPR}$$

The resulting STDR is the converse of the confidence level that the auditor will use for his/her substantive sample. For example, if STDR is determined to be 15%, the auditor will use an 85% confidence level for his/her sampling procedures.

### 7.8.7 Considering the assurance achievable from each audit step

Auditors are not required to develop the detailed audit programmes during the Planning Phase. However, the auditor should give some consideration to the types of procedures, and the assurance that can be derived from each procedure, in order to make a reasonable determination of the optimum combination of sources of audit assurance.

The amount of assurance that can be derived from each procedure depends on the nature of the test and the evidence that will be collected. The auditor should have a sound understanding of:

- The nature of evidence;
- What constitutes appropriate quality and quantity of evidence; and
- The most appropriate methods of collecting evidence.

### **7.8.8 Considering staffing, budgeting and timing of the audit**

The staffing, budgeting and timing of the audit are all matters to be dealt with in detail at the detailed planning stage. They are discussed in detail in Chapter 8.

However, the auditor should give these matters some consideration during the general planning phase. There is no point coming up with an optimum combination of tests of internal control, analytical procedures and substantive tests of details unless adequate time or resources are available.

*Staffing.* Unless an audit is appropriately staffed, the benefits of good audit planning can be lost. Persons involved in the general planning phase need to make sure that there are staff members available who have the audit skills required to perform the work efficiently and effectively.

For example, the auditor may determine that the most efficient audit approach would be to place high reliance on internal controls and to use regression analysis. However, unless the audit can be staffed with people capable of doing a detailed evaluation of an internal control structure and using a regression analysis software package, this approach is not practicable.

*Budgeting the work.* DAGP has finite resources, so it is important to estimate the time required to perform the audit under each combination of tests.

Each financial audit will require a minimum amount of resources. DAGP needs to ensure that the required resources are allocated. Since the resources required for compliance with authority work can be more flexible than those required for financial certification, the Director may have some scope for reallocating resources in response to certification audit demands.

*Timing of the work.* Most government entities have the same year-end date (30 June). To keep audit staff busy throughout the year, and complete the audit of the financial statements on a timely basis after the year-end date, it is often appropriate to perform some of the work in advance of the year-end date. This should be taken into account when scheduling audit activities.

*Supporting software.* Audit management software can be used to assist in the staffing, budgeting and timing of the audit work.

### **7.8.9 Re-assessing the general planning decisions for individual audits**

Before completing the general planning phase, the auditor should consider whether decisions made in later steps in the phase indicate that changes are needed to decisions made earlier in the phase. For example, the assessment of inherent risk and control risk may result in the auditor re-estimating the amount required for the expected aggregate error. Similarly, staffing and timing issues may affect the auditor's ability to use the optimum mix of tests of internal control, analytical procedures and substantive tests of details.

In addition, audits cannot be planned in isolation. Each audit directorate needs to consider how best to utilise all of its staff members on all of its audits in the most efficient and effective manner. Planning decisions should also be re-assessed in later stages of the audit.

## 7.9 Reliance on other auditors

A key factor to consider in the general planning phase is the extent to which the auditor can rely on the work of internal auditors.

Reliance on internal auditors can affect the work required to update the understanding of the internal control structure. It will also likely affect the assessment of control risk.

In addition, the ability to rely on internal auditors will likely affect the optimum mix of tests of internal control, analytical procedures and substantive tests of details.

### 7.9.1 Internal auditors

Internal auditors have an independent appraisal function within their organisations. As such, they are part of the entity's internal control structure.

In general, the relationship between DAGP and the internal audit community should be one of cooperation and professional reliance. Coordination of work can ensure adequate audit coverage, while at the same time minimising duplicate efforts.

The coordination and cooperation between DAGP and each internal audit organisation can be enhanced by:

- DAGP and the internal audit unit coordinating their audit effort, which in turn requires each:
  - To have knowledge of the planned audit coverage of the other; and
  - To the extent possible, to amend its plans to better coordinate the effort.
- Having access to each other's audit programmes and internal control questionnaires;
- DAGP having access to the working papers of the internal audit organisation;
- Having an exchange of audit reports and management letters;
- Having a common understanding of audit techniques, methods, and terminology; and
- DAGP relying, to the extent possible, on the audit work of the internal auditors, and thus reducing the amount of additional testing required by the DAGP auditors.

Coordination of effort requires that DAGP and the internal audit staff meet well before the commencement of specific audits to jointly plan their work for the following year. During these meetings, DAGP could, for example:

- Discuss areas where it would like to rely on the work of internal audit;
- Provide the internal auditors with its basic planning parameters – materiality, audit risk, sources of audit assurance, etc.;
- Provide the internal auditors with an audit programme, summary of unadjusted differences and other forms and checklists for the internal auditors to complete; and
- Discuss the timing of the work and any required deadline dates.

One of the roles of internal audit is to provide management with an assessment of the adequacy and effectiveness of the internal control structure and the extent to which it can be relied upon. Auditors from DAGP should consult with the head of the internal audit

organisation to determine how much audit work internal audit has performed on the internal controls. Wherever possible, the DAGP auditors should rely on the work of internal audit.

Just like any other control, the unit's work needs to be tested before it can be relied upon. DAGP auditors should consider examining the systems and procedures that the internal audit unit has in place to ensure that its work is performed to the required standards. These systems and procedures would include the unit's quality assurance procedures, hiring policies and training programme. The DAGP auditors may also wish to re-perform some of the work performed by internal audit.

Sometimes the external auditors use internal auditors to perform some of the external audit work. In cases such as this, the internal auditors are effectively acting as members of the external audit team. Their work should be supervised and their files reviewed just like the work of any other member of the team.

## **7.10 Documenting strategic planning decisions**

### **7.10.1 The need to document planning decisions**

The auditor's documentation, in the form of audit files, is collectively referred to as the "working papers".

Paragraph 3.5.5 of DAGP's auditing standards states, "*Auditors should adequately document the audit evidence in working papers, including the basis and extent of the planning, work performed and the findings of the audit.*"

Documentation of the planning decisions is discussed in detail in Chapter 8. At the end of the detailed planning stage, all steps in the planning process should be complete and adequately documented.

It should be noted that the documentation of the audit planning phase should not wait until the detailed planning steps are complete. The work done in each step of the audit planning phase should be fully documented as soon as the work has been completed.

At the end of the audit planning phase there should be documentation in the planning file and in the permanent file of all of the decisions made during the general planning phase. In addition, the relevant sections in the audit planning memorandum should be completed. The individuals completing the detailed planning phase can then make use of all of this material.

## **7.11 Application to Government-wide Audits**

### **7.11.1 Sample selection**

As noted earlier, the auditor uses one overall materiality amount for the audit, and does not need to allocate it to each grant, component, location, etc. In addition, this one overall materiality amount is used when determining minimum sample sizes for the audit of each component, and each specific financial audit objective and related compliance with authority objective. (Note: this is not to limit the discretion of DAGP to perform more rigorous sampling as it sees fit, especially for compliance with authority audit work).

For government-wide audits, the materiality amount will be established by a central DAGP team that is responsible for the overall planning, performance, evaluation, reporting and

follow up of the audit. For the audit of the financial statements of an individual government agency, the materiality amount will usually be set by the audit director or a more senior staff person.

Each ministry, department etc. performs accounting functions at different locations – the Account General Pakistan Revenues, principal accounting officers in the ministry or department, DAOs, DDOs, etc.

Using one overall materiality amount ensures that every grant that is greater than the materiality amount, and every location with assets, liabilities, revenues or expenditures greater than the materiality amount will be virtually certain to have at least one transaction selected for audit. Similarly, each grant and each location with assets, liabilities, revenues or expenditures greater than one half of the materiality amount will also be likely to have at least one transaction selected for audit. It is possible that sampling techniques will not select items from all DDOs, DAOs etc. (DAGP has full discretion to extend sample selection to include items from every DDO and DAO if it is considered necessary).

In addition, for the audit of the Federal Government, a province or a district, the auditor is again using a single materiality amount for each audit entity, and that amount is based on the assets, liabilities, revenues or expenditures of that entity as a whole, not each of the sub-entities, such as ministry or department, within the audit entity. Therefore it is possible that sampling techniques will not select audit items from some of the smaller sub-entities. This is logical, since sub-entities that are small relative to materiality are not significant from a financial audit perspective.

However, with direction from DAGP, auditors have the freedom to extend the scope of their audit to extend audit coverage to as many sub-entities as deemed appropriate, and the coverage within each sub-entity, even 100% sampling, is also discretionary. Auditors often accomplish this by developing a list of minimum procedures to be applied at specified sub-entities that is applied over and above the samples determined by sampling techniques. Procedures that can help identify additional areas where coverage would be useful include:

1. Updating knowledge of the business by looking for new legislation, reviewing minutes etc.,
2. Reviewing the basic control environment;
3. Performing analytical procedures on each line item in the financial statements (including statement of appropriations); and,
4. Exploring for significant events and transactions after the year-end cut-off date.

The auditor could also select additional transactions at random and perform various tests on those items. Bear in mind that the most useful test, given the small size of some sub-entities relative to materiality, is to look for unrecorded transactions rather than errors in recorded transactions. In particular, the auditor would look for unrecorded expenditures that could be hiding over-expended appropriations.

The choice of which grants, locations, ministries or other sub-entities on which to perform these discretionary procedures is based primarily on the auditor's professional judgement and knowledge of the entity. The auditor should consider the following:

- The grants, locations, ministries, etc. suspected of significant inherent and control risk;
- Sub-entity headquarters where records are kept and where management likely exerts the most influence over transactions;

- All individually significant events, transactions or sub-entities.

In addition to extending the coverage of planned financial audit procedures, the auditor may also decide to conduct additional audit work to review compliance with authority, internal controls, performance and so on.

### **7.11.2 Coordination**

It is not feasible for each audit directorate to plan its portion of the audit of the Federal Government, province or district in isolation. The materiality amount and planned precision value need to be set and the audit work on each component (e.g. line item in the financial statements) should be coordinated across ministries, departments, agencies, etc.

A single grant may be spread across a number of departments, and one DAO may manage more than one grant. It is essential that each grant is subject to an appropriate level of investigation. DAGP has created a central team responsible for audit planning, performance, evaluation, reporting and follow up of each government wide audit. For the annual audit of the financial statements of the Federation, the central team is responsible for:

- Setting basic planning parameters (materiality, audit risk, planned precision, components to audit, etc.);
- Setting inherent risk, control risk, other substantive procedures risk and substantive test of details risk for each component and audit objective, compliance objective, error and irregularity;
- Determining optimum mix of tests of internal control, analytical procedures, and substantive tests of detail for each component and audit objective, compliance objective, error and irregularity;
- Drafting audit programmes, forms and checklists to be used by audit teams;
- Performing overall error evaluation; and
- Reporting the results of the audit.