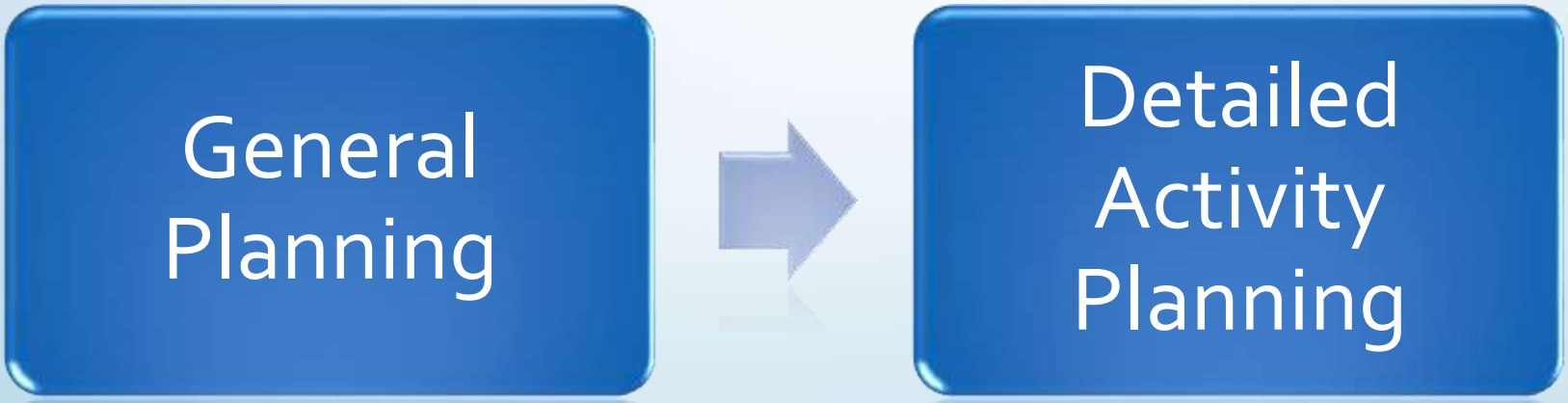
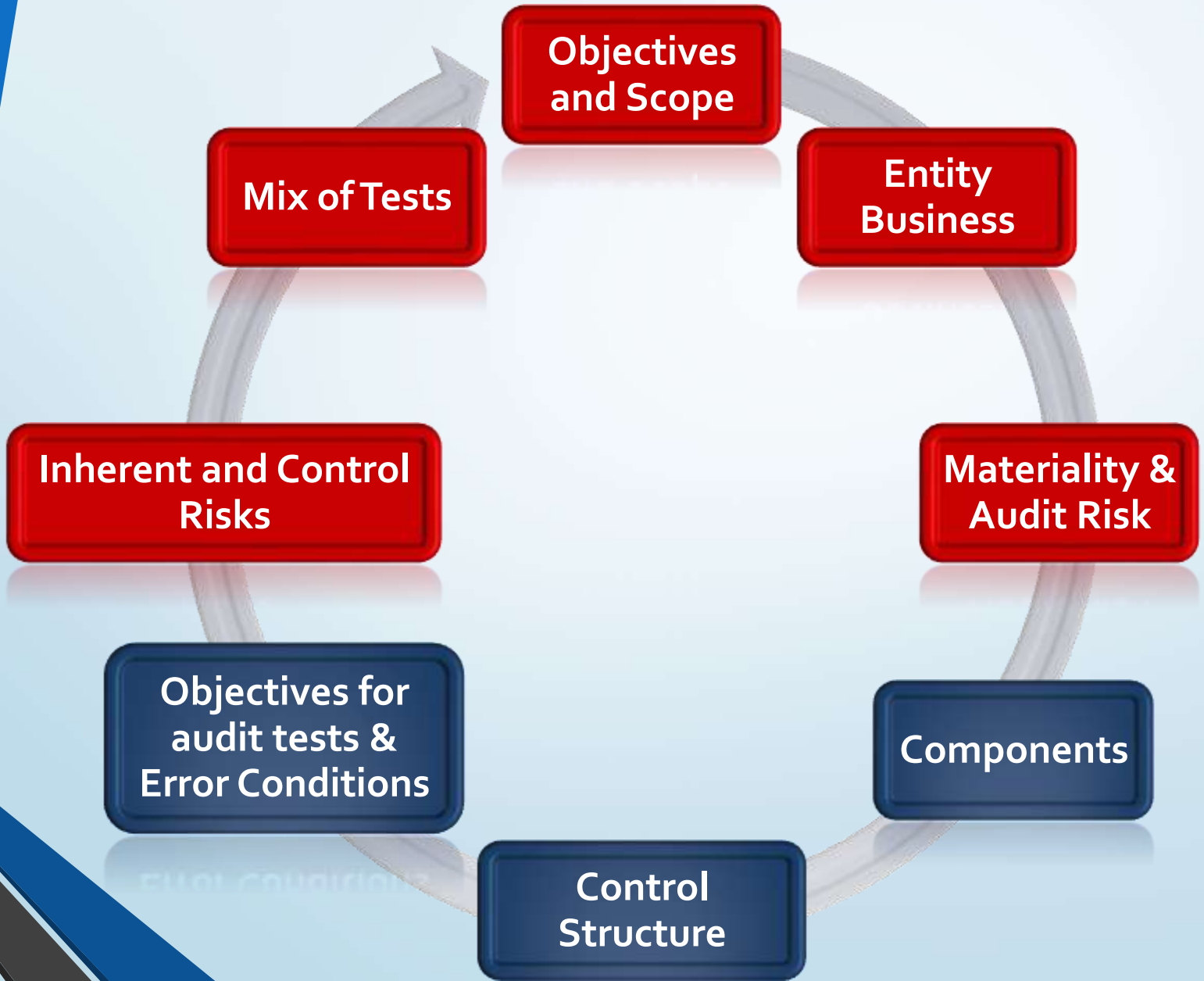
Financial Audit Planning Steps

Planning Phases



GENERAL PLANNING STEPS



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 fulfill multiple audit objectives, so it is important that the audit is well-planned in terms of audit objectives and audit scope.

Overall Audit Objectives

Overall Audit Objectives

To express an opinion on financial statements:

- 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:

- 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 needs to look for will reflect the objectives of the compliance audit.

For compliance with authority audit work with no expression of an opinion:

- the auditor need not plan the audit to obtain a specified minimum level of overall audit assurance.

Performance Audits:

- 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.

Audit Scope

The overall audit scope:

- the total population on which to express an opinion,
  - from which to select transactions, etc.

Audit Scope

In some cases, the scope of the audit can be at the auditor's discretion, or can be negotiated with entity management.

- For example, a SAI 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 SAI should defer its audit by a year so that the two audits could be coordinated.

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.

- 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.

Step 2 – Understand the Entity's Business

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.

Information Required

- 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).

Use of the Information

Materiality:	• an understanding of the users of the entity's services and the size of the entity is needed to assess materiality;
Components:	• 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;
Inherent Risk:	• 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.

Step 3: Materiality and AR

DEFINITION

Materiality—Information is material if its omission or misstatement could influence the **economic decisions** of users taken **on the basis of the financial statements**.

Materiality should be determined from the **user's point of view** and not from the auditor's.

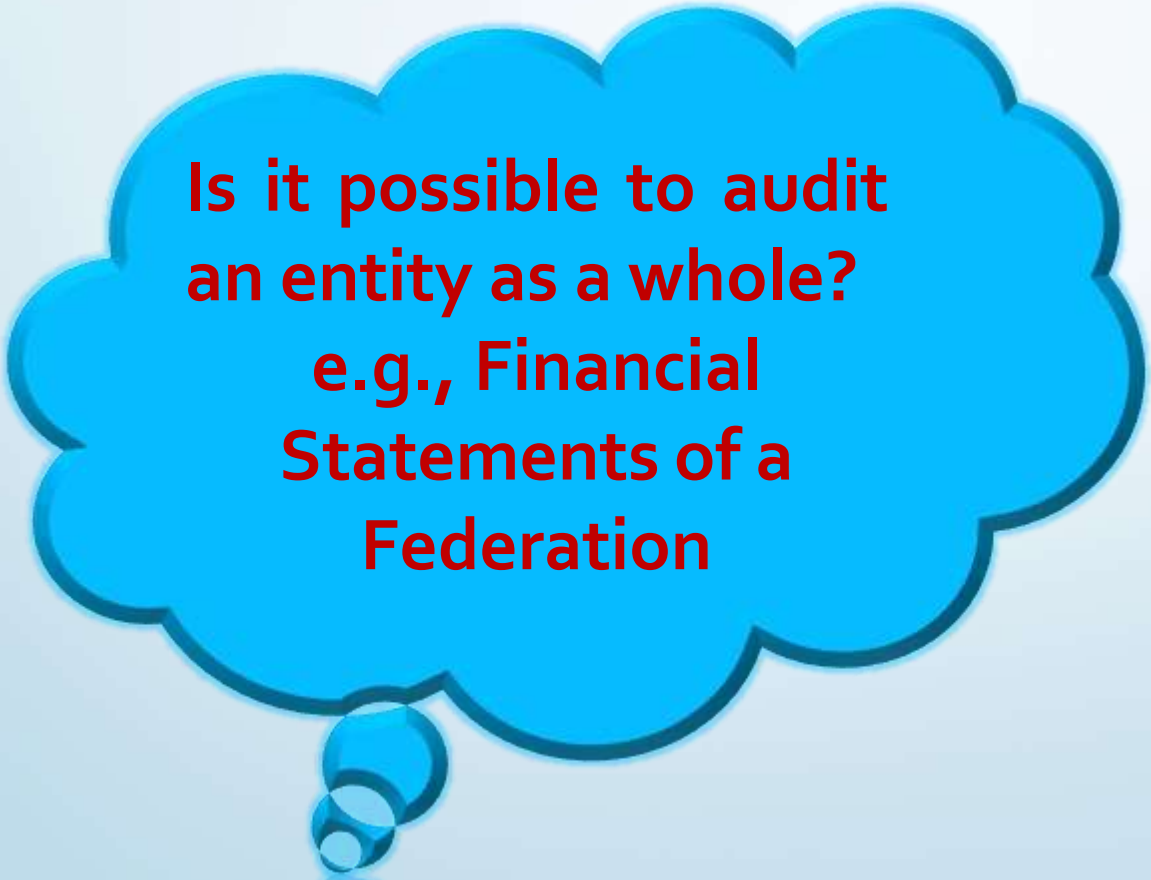
Audit Risk - Definition

Overall Audit Risk is the maximum risk that the auditor is prepared to assume that error in the financial statements aggregating to more than **materiality** will remain **undetected** at the end of the audit.

STEP 4

DETERMINE COMPONENTS

COMPONENTS


Is it possible to audit an entity as a whole? e.g., Financial Statements of a Federation

FS COMPONENTS – LINE ITEMS

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.

CONSIDERATIONS FOR COMPONENTS

The auditor selects the grouping that makes it the *easiest* to AUDIT.

The auditor would then need to perform additional procedures to ensure that the amounts reported in the other groupings are also presented fairly.

expenditures are grouped by both *ministry* and by *object element*. If the auditor chooses "object element", means payroll/operating expenditures are not materially misstated, etc. Additional audit procedures are required to ensure that the total expenditures of each ministry is also not misstated.

SUB-COMPONENTS

Where the inherent risk and control risk for part of a component are significantly different than for the rest of a component

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.

SUB-COMPONENTS – INDIVIDUALLY SIGNIFICANT TRANSACTIONS AND EVENTS

Very large transactions and even

- These are large enou that, should they be in error, the e or could b ficant.
- The loes not ant to risk failing to fi ons and events.

These are checked 100%

High transacti and even s

s that, because of high risk of being in error.

or in each one of these transactions events may not be significant, the high likely error rate in these transactions and events could result in a significant error in total.

INDIVIDUALLY SIGNIFICANT TRANSACTIONS AND EVENTS

Very large transactions and events

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

High risk transactions and events

- **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.**

INDIVIDUALLY SIGNIFICANT TRANSACTIONS AND EVENTS

Not as Separate Component

- These transactions and events are normally not treated as separate components. Rather, they are audited as part of the work performed on other components.

As Separate Component

- Sometimes 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.

Step 5 Understanding Controls

DEFINITION

INTOSAI: plans and actions of an organization, 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, and 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.

CATEGORIES OF CONTROLS

1. INPUT VS OUTPUT

Input controls: are controls over the initial input of data. They include'

- password controls to prevent unauthorized personnel from inputting transactions.

Output controls: are controls over the output from systems. They include;

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

2. INDEPENDENT VS INTERRELATED

Independent Control: is a control that may work on its own. For example

- a reconciliation may be a powerful control in its own right.

Interrelated control: is a control that is dependent on the effectiveness of other controls to achieve the desired overall objective. For example

- an input control will only be effective if the entity also has adequate controls over data processing and output.

3. MANUAL VS ELECTRONIC

Manual controls: are operated by staff.

can be affected by human errors of judgment, misinterpretation, carelessness, fatigue, and distractions.

Electronic controls: are built into computer programmes

If the systems are properly designed, installed and tested these are more reliable.

however problems with the software are difficult to detect and expensive to correct.

4. GENERAL VS APPLICATION

General controls: are applicable to the 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 authorized, complete and accurate, such as

- not accepting other than specified numbers for a particular field or code, e.g., not excepting transactions prior to certain date or age above retirement age.

5. 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. Examples,

- 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.*
- when management and staff of an entity follow sound control principles based on experience and are not not documented. The controls may be lost when staff turnover occurs.

6. PREVENTIVE VS DETECTIVE

Preventive controls: prevent errors from occurring. Example;

- Most data entry controls are preventive controls.

Detective controls: detect errors that have occurred.

- Most output controls and reconciliation controls are detective controls.

It is generally less costly to prevent an error than it is to detect and correct it after the fact. Therefore, preventive controls are usually less costly to use than detective controls.

7. COMPENSATING CONTROLS

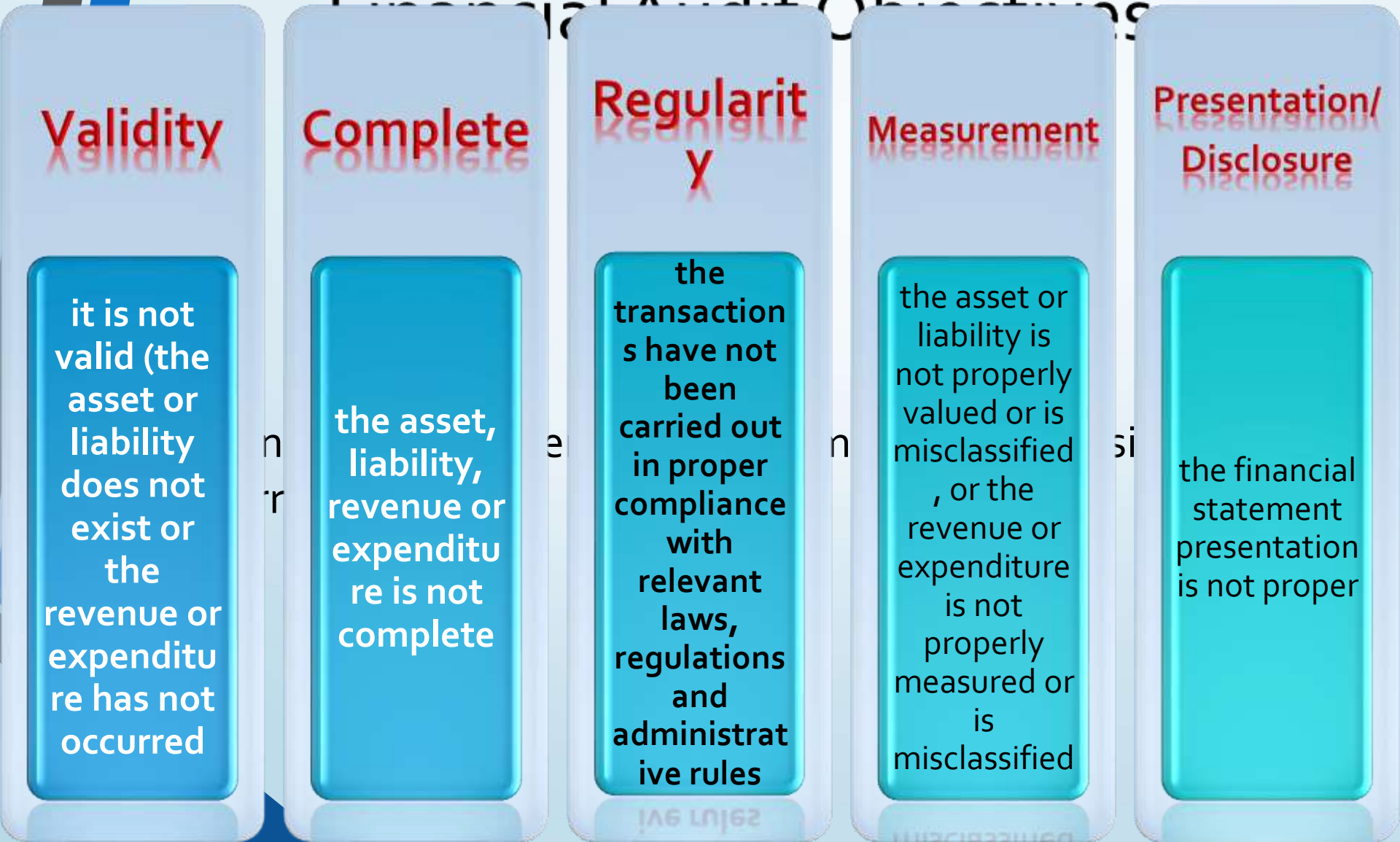
These controls detect errors that occur at earlier control points.

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.

Step6: Specific Audit Objectives and Identifying potential error/irregularity conditions

Financial Audit Objectives



Validity	Complete	Regularity	Measurement	Presentation/ Disclosure
This could be due to, inter alia, ghost workers on the payroll.	Employees have not been paid, or the payments have not been recorded.	Employees have not been hired after approval of competent authority	paying employees more or less than they should be paid, or the amounts being recorded being more or less than the actual payments	due to the failure to disclose all of the information called for in the New Accounting Model

Related Compliance with Authority

Reviewing compliance with laws and regulations is required because decision makers need to know if

the laws and regulations are being followed	whether they are having the desired results	if not, what revisions are necessary

Identifying Potential Error Conditions

- **The ways in which a monetary error can occur in the financial statements, or an applicable authority may not be complied with.**

Potentially Big Error Conditions

Occurrence Chance

- Only those conditions are considered for which chance of occurrence is considerable.

Size of Error/Irregularity

- the maximum possible error that could result is relatively large in relation to the materiality amount

Subsequent Sessions

Step 7: Determining Inherent and Control Risks

Step 8: Determining Mix of Audit Tests

Thank you