

AUD-2

Internal Control

Internal Control

The **second standard of fieldwork** states:

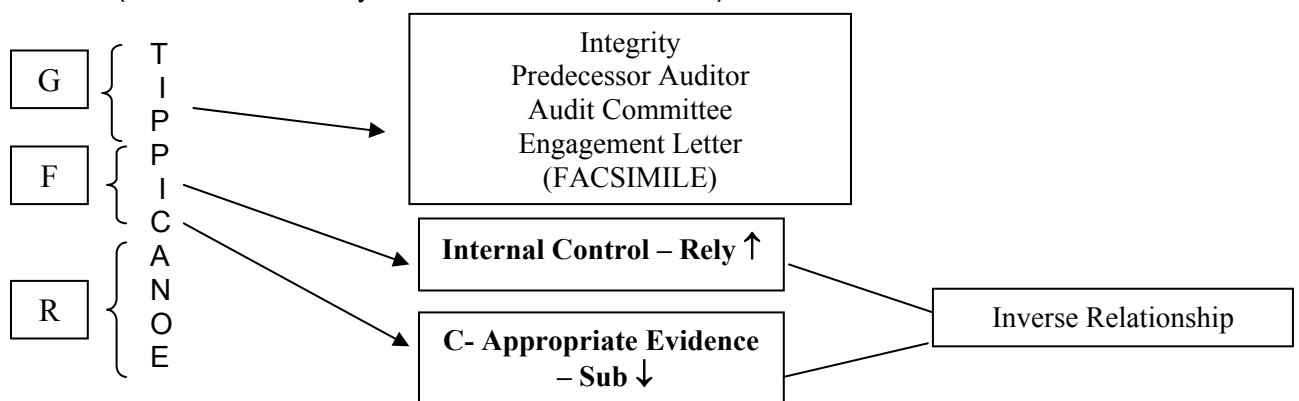
“The auditor *must* obtain a sufficient **understanding** of the entity and the **environment**, including its **internal control**, to assess the risk of material misstatement (RMM) of the financial statements whether due to **error or fraud**, and to design the **nature, timing, and extent** of further audit procedures.”

For Financial Statement audits (Nonissuer), the auditor expresses an opinion on the client's financial statements, not on their internal control structure. The reason the auditor is interested in the client's internal control structure is the inverse relationship between Control risk (RMM) and Detection risk: the stronger the internal control structure, the less substantive testing the auditor will have to perform. The auditor cannot finalize the audit program until the level of Control Risk (RMM) has been assessed and an acceptable level of detection risk determined. To assess Control Risk (RMM) for specific financial statement assertions at less than the maximum, the auditor is required to obtain evidence that the relevant controls operated effectively during the **entire period** (including during the course of the audit engagement) upon which the auditor plans to place reliance on those controls.

For Audits of Public Companies (Issuer), The Sarbanes-Oxley Act of 2002 created a requirement for an integrated audit of SEC registrants that provides assurance about the **fairness of financial statements and about the effectiveness of internal control over financial reporting (ICFR)**. The financial statement audit portion of the “*integrated audit*” is similar to any other financial statement audit, but its integrated nature means that auditors rely much more on internal control and less on substantive procedures. The objective of the tests of controls in an audit of internal control over financial reporting is to obtain evidence about the effectiveness of controls to support the auditor's opinion on the company's internal control over financial reporting. The auditor's opinion relates to the effectiveness of the company's internal control over financial reporting **as of a point in time** (“point of time” defined as *the last day of the fiscal period, it is this date on which the auditor concludes as to the effectiveness of internal control*) and *taken as a whole*.

As a result, the auditor is looking for the presence of useful controls: the strengths in the system. The system is primarily formed by those controls designed by management that relate to the financial statement assertions and which are meant to produce **accurate financial records** and **safeguarding of assets**. Those controls designed to enable adherence to laws and regulations and promote efficiency in the organization are usually not relevant to the financial statement assertions.

10 GAAS (Measure of Quality of Auditor – TIPPICANOE)



The most commonly used framework to benchmark internal controls in the US is *Internal Control – Integrated Framework* developed by COSO. COSO describes internal control as:

A process, effected by the entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives in the categories of (1) Accurate and reliable financial reporting, (2) Compliance with applicable laws and regulations, and (3) Effectiveness and efficiency of operations (ACE).

- So, Management is responsible for the establishment and maintenance of Internal controls. We want Reasonable assurance that Internal controls are achieving certain **Objectives (ACE)**:
 - **Accurate & Reliable** financial reporting
 - **Compliance** with laws and regulations
 - **Effectiveness** and efficiency of operations

The mnemonic ACE will remind management that it should try to establish a strong internal control structure so as to have an ACE in the hole.

The primary interest of the outside auditor is in the first objective, accurate and reliable financial reporting which relate to the fair presentation of the financial statements being audited. The second goal, compliance with laws and regulations, is primarily relevant to **compliance auditing**, which may occur in connection with audits under government auditing standards. The third goal, promoting effectiveness and efficiency of operations, is of little interest to an outside auditor except in the case of rarely-performed **operational audits**.

SAS 109 (AU 314) The auditor should obtain an understanding of the **5 components of internal control** under COSO in order to evaluate the design of relevant controls and determine whether they have been implemented, assess the risk of material misstatement and design the nature, timing and extent of further audit procedures.

Elements of internal control: **(CRIME)**

- **Control activities**
 - Policies and procedures that help ensure that management directives are carried out.
 - **Performance reviews** – Actual vs. budget, P/Y, financial to non-financial
 - **Information processing** – (IT) General vs. Application controls
 - **Physical controls** – Access to assets
 - **Segregation of duties** includes assigning different people the responsibilities of **authorizing** transactions, **recording** transactions, maintaining **custody** of assets, and performing **comparisons**. It is intended to reduce the opportunities to allow any person to be in a position to both *perpetrate and conceal errors or irregularities* in the normal course of their duties (**ARCCS**).
 - **Authorization** of transactions
 - **Recording** (posting) of transactions
 - **Custody** of assets
 - **Comparisons**

- **Risk assessment**

- An entity's risk assessment for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation of financial statements that are fairly presented in conformity with GAAP. Risk assessment includes risks that may affect an entity's ability to properly record, process, summarize, and report financial data. Risk assessment, for example, may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements.

Risks relevant to financial reporting include external and internal **factors** such as the following:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New lines of business, products or activities
- Corporate restructurings
- Foreign operations
- Accounting pronouncements

- **Information and communication**

- Refers to the I.D, retention, and transfer of information in a timely manner allowing personnel to perform their responsibilities.
 - **Info system** consists of the methods and records used to *record, process, summarize and report* Co.'s transactions and to maintain accountability for the related accounts
 - **Communication** involves establishing individual duties and responsibilities relating to internal control and making them known to involved personnel.

- **Monitoring**

- An important management responsibility is to establish and maintain internal control. Management monitors controls to consider whether they are operating as intended and that they are modified as appropriate for changes in conditions. Monitoring is a process that assesses the quality of internal control performance over time.

- **Control Environment (CHOPPER)**

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the following:

- **Commitment to competence** - Effective control requires a sincere interest on the part of the employees in performing good work.
- **Human resource policies & practices** - A company can minimize the control difficulties created by new employees by sound hiring and training policies for employees.
- **Organizational structure** - A company that operates all over the world has different internal control problems than one operating entirely within a single building.

- **Participation of those charged with Governance** - An audit committee of the board of directors that actively monitors the internal audit function produces a more attentive management on such matters.
- **Philosophy of management & operating style** - The belief (or lack of it) in the importance of internal control by management will affect the seriousness with which it is taken by the rest of the employees. This is especially the case when decision-making in the company is dominated by a single individual.
- **Ethical values & Integrity** - Honest employees will be less likely to cause internal control difficulties related to fraud and improve the opportunity for those resulting from errors to be effectively detected.
- **Responsibility assignment** - The manner in which authority, responsibility and accountability is assigned to different employees determines the controls that will be needed. Again, the domination of decision-making by a single individual holds significance, since such power makes it extremely difficult for internal control to be trusted.

The mnemonic **CRIME** reminds management that it would be a crime not to consider all of the internal control elements when designing the system.

Understanding the internal control structure SAS 109 (AU 314)

An auditor performs the following procedures to obtain an understanding of internal control:

- Step 1 - Obtain an understanding of the design of internal control (perform risk assessment procedures - CRIME)
- Step 2 - Document the understanding of Internal Control
- Step 3 - Assess Risk of Material Misstatement (RMM = IR x CR)
- Step 4 - Perform tests of controls
- Step 5 - Reassess risk of Material Misstatement and evaluate results.
- Step 6 –Document conclusions and complete the planned substantive procedures

1. Understand the design of CRIME (perform *Risk Assessment Procedures*) (what is the form?)

Have the controls been **IMPLEMENTED** (put into use?). To evaluate the implementation of a control means to determine whether a control is actually being used by the entity. The auditor first considers the design of the control. If the control is improperly designed, it may represent a material weakness in the entity's internal control.

Risk assessment procedures are used to obtain an understanding of the entity and its environment, including its internal control (CRIME), in order to assess the risk of material misstatement (RMM) and to design the nature, timing and extent of further audit procedures.

Risk assessment procedures to obtain an Understanding include:

- *Analytical procedures* (Using high-level data)
- *Inquiries* of management and staff
- *Inspection* of documents and records
- *Observing* the applications of specific controls

The knowledge obtained through risk assessment procedures is used to:

- Identify the types of potential misstatements (Errors or Fraud).
- Consider factors that affect the risk of material misstatements.
- Design tests of controls and Substantive procedures

- As part of obtaining an understanding of internal control sufficient to plan the audit, the auditor should evaluate whether the client's programs and controls that address the identified risks of material misstatement due to fraud have been suitably designed and implemented.
- Determine if these have been **Implemented (Placed into operation)**.
 - Understanding **doesn't** require evaluating their **operating effectiveness**.

The goal of this understanding is to identify those controls that might reduce the risk of misstatements. If these controls can be relied on, the auditor will be able to reduce substantive testing.

Notice, however, that the auditor is only trying to determine what controls have been **implemented** (are being used), and is **not** determining whether the controls have been **operating effectively**. The latter is only necessary in a financial statement audit if the auditor plans to rely on the controls. The auditor's main concern is whether, and how, a specific control prevents, detects, and corrects material misstatements in relevant assertions. Once the auditor has gained an understanding of the internal control structure, they may decide to assess the Risk of Material Misstatement high (not rely on internal control), in which case there is no point in determining whether the controls are effective.

The techniques available to the auditor to gain information about a client's internal control structure include:

- **Prior audits** - Reviewing audit documentation that document the internal control structure of the client in prior years.
- **Inquiry** - Asking management and other client personnel to describe the controls that they are currently using.
- **Inspection** - Examining documents that are used in internal control, such as authorization forms and procedures manuals.
- **Observation** - Watching employees perform their jobs.

Keep in mind that the auditor is initially interested in the form, but is ultimately interested in the **substance** of the controls. Often, inquiry and inspection will provide the auditor with information about controls that have been designed, but **observation** will reveal that these controls aren't actually being enforced by management. Observation is especially critical in determining whether controls involving **segregation of duties** are being implemented in practice, and not just in theory.

2. Document understanding of Internal Control

The auditor's documentation of their understanding of internal control should include the key elements of the understanding obtained regarding the 5 components of I/C (CRIME), the sources of information from which the understanding was obtained, and the risk assessment procedures performed. The form is influenced by the size and complexity of the entity. There are different techniques for documenting the auditor's understanding of the internal control structure (**FIND**):

- **Flowchart** - The auditor prepares a visual depiction of the internal control structure. This requires knowledge of specialized symbols but does the best job of giving the auditor a sense of the flow and sequence of transactions in the client entity. Testing on the CPA exam has been limited to reading flowcharts and then answering conventional questions about strengths and weaknesses in the internal control structure, and has

never involved their preparation. Historically, exam questions have been written so that the candidate could understand flowcharts provided even if they had no prior knowledge of the standard meaning of the various symbols, and we do not suggest using your valuable study time in an attempt to learn the symbols.

- **Internal Control Questionnaire (ICQ)** - A series of yes/no questions are prepared and answered by the auditor regarding the internal control structure. Each question is designed to identify a potentially useful internal control element that might be relied upon if it is operating effectively. This is the most structured of the approaches, is easiest for an inexperienced staff member in an audit to utilize, and is a very popular area of testing on the CPA exam.
- **Narrative or Memorandum** - The auditor provides a detailed written description of the internal control structure. This approach is extremely cumbersome and provides the auditor with no structure or guidance, so it is not commonly used, and it is virtually never tested on the CPA exam. It is sometimes called the narrative approach.
- **Decision table/tree** - Parts of an internal control structure may require a client employee to choose from several alternative actions depending on the conditions faced, and documenting such activities. This may best be accomplished by preparing a decision table that lists each possible condition and the actions that will result from each (depicts the logic of an operation or process). It uses Yes/No questions and each answer will direct the user to the next relevant question. This is, however, a limited tool that cannot effectively document the entire structure.

NO – RMM ↑ (Sub Approach)

3. Assessing Risk of Material Misstatement (RMM)

YES – RMM ↓ (Combined Approach)

The auditor should perform the risk assessment to identify and assess the risks of material misstatement at the financial statement level and at the relevant assertion level for classes of transactions, account balances, and disclosures.

The auditor may use either a *substantive approach*, in which substantive procedures are emphasized, or a *combined approach*, in which both tests of controls and substantive procedures are used.

- The auditor needs to
 - Identify the risks
 - Relate the identified risks to the types of potential misstatements that could occur at the relevant assertion level
 - Consider whether the risks are so significant that they could result in a material misstatement of the financial statements
 - Consider the likelihood (probability) that the identified risks could result in material misstatements on the financial statements.

If the risk assessment is based on an expectation that controls are operating effectively, the auditor should test the operating effectiveness of controls (T-of-C) that have been determined to be suitably designed to prevent or detect material misstatements.

- Intend to Rely?
The risk assessment may **NOT** include an expectation that controls operate effectively when (*Substantive approach*):

- Controls appear **inadequate / Ineffective/ weak**
- Auditor believes that performing extensive substantive procedures is likely to be more *cost effective* than performing tests of controls. (**Cost/benefit – inefficient**)

If the controls **appear effective**, tests of controls will be performed when (*Combined approach*):

- the auditor's risk assessment includes an expectation of **operating effectiveness of controls** because the likelihood of material misstatement is lower if the control operates effectively (*Cost effective*) or
- When **substantive procedures alone** do not provide sufficient audit evidence.

Since tests of controls alone are not normally sufficient upon which to base an audit opinion, the further audit procedures will be composed of a *combination* of tests of controls and substantive procedures. Thus, the decision to perform tests of controls will be made when the auditor believes that a combination of tests of controls and a decreased scope of substantive procedures is likely to be more cost effective than performing more extensive substantive procedures. The overall approach here, as it relates to controls is to

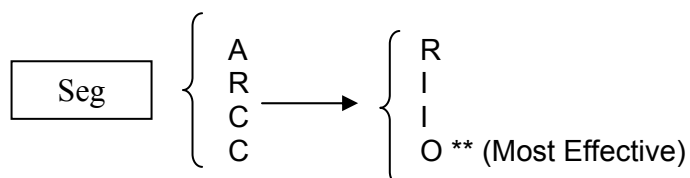
- Identify controls that are relevant to specific assertions that are likely to prevent or detect material misstatements, and
- Perform tests of controls to evaluate the effectiveness of those controls.

4. Tests of controls – To test the effectiveness of the design and operation of a control (what is the substance?). The auditor must consider how the control was applied, the consistency with which it was applied and by whom it was applied.

- Testing the Cycles for **ARCC's** by doing **RIIO**

There are 4 *Procedures* for testing controls.

- **Reperformance** - The auditor applies the control that the client personnel presumably performed earlier. For example, if the payables clerk was supposed to match vendor invoices with purchase orders and receiving reports before preparing a voucher for payment, the auditor might pull a sample of payment vouchers that were generated during the year and attempt to locate the appropriate supporting documents and match them.
- **Inspection** - The auditor examines controls, documents and reports that provide documentary evidence. For example, the auditor might examine client records documenting the use of computer programs.
- **Inquiry** - The auditor asks client personnel involved in controls to state how effectively certain controls were enforced. For example, the auditor might ask the accounting personnel if they handled any cash or signed checks in the course of the year.
- **Observation** - The auditor watches client personnel performing their regular functions to see if they follow the controls that were designed and implemented. For example, the auditor might observe the distribution of pay checks to see if appropriate procedures for verifying employees are being followed.



If the auditor plans to use audit evidence about the operating effectiveness of controls obtained in prior audits and the controls have not changed since they were last tested, the auditor should test the operating effectiveness of such controls at least **once in every three years**.

5. Reassess RMM to determine DR

Based on the results of the tests of controls the auditor will determine whether it is necessary to modify the scope of substantive procedures. If tests of control reveal that the system *operates as expected*, there will generally be no need to change the scope of planned substantive procedures. Conversely, if the system does not operate as effectively as expected, the scope of substantive procedures for the relevant assertions involved will increase (thereby decreasing detection risk).

- DR tells you how much substantive testing to do
- Must do substantive testing (adjust Audit Program for Substantive tests)
- $AR / (IR \times CR) = DR$

6. Document Conclusions

The auditor is *required* to communicate significant deficiencies and material weaknesses to management and those charged with governance. The basis for risk assessment must *always* be documented. The auditor needs to document:

- The assessment of the risks of material misstatement at the financial statement and relevant assertion levels;
- The *basis* for that assessment;
- Significant risks identified and related controls evaluated;
- Risks identified that require tests of controls to obtain sufficient audit evidence and the related controls evaluated.

Sarbanes-Oxley Act (SOX)

SOX created a variety of new regulations and eliminated a significant portion of the accounting profession's system of self regulation. Some new issues include:

- Section 302 makes officers responsible for maintaining effective internal controls and requires signing officers to disclose all significant internal control deficiencies to issuer's auditors and audit committee.
- Officers are also required to report any fraud (whether material or not) involving management or employees with role in internal controls.

Basic concepts

Regardless of the good intentions of management, even a strong control environment combined with excellent control activities is subject to certain **inherent limitations** (COCO):

- **Collusion** - Control activities that depend on segregation of duties will not be effective if those engaged in the segregated functions conspire together.
- **Override by management** - Since management designs and implements the system of internal control, it is in a position to override it, so that even an effective internal control structure cannot be expected to prevent intentional misbehavior by management. This is one of the reasons the auditor must establish the integrity of management before accepting the engagement. It is also important to establish whether employee personnel have ever been asked to override systems of internal control by management.

- **Competence** - If control procedures are erroneously applied, they will not be effective. Internal control cannot be expected to prevent mistakes in human judgment (misjudgment).
- **Obsolescence** - A good internal control structure may cease to be effective due to changes in the company's operations or size.

It is essential to keep in mind the concept of **reasonable assurance** as it relates to internal control. Even were it possible to design a perfect system of internal control, management would not do so, since there are costs involved in any action, and the costs of the internal control structure should not exceed the benefits. As a result, management may sometimes reasonably refuse to remedy a deficiency in internal control that it knows exists.

SAS 99 (AU 316) requires the auditor to respond to management override of controls – Because management is often in a position to override controls in order to commit financial-statement fraud, the standard includes procedures to test for management override of controls on every audit. It should be noted that SAS 99 states that even a properly planned and performed audit may not detect a material misstatement resulting from fraud because of (1) concealment aspects of fraudulent activity, including the fact that fraud often involves collusion or falsified documents, and (2) the need to apply professional judgment in the identification of evaluation of *fraud risk factors* and other conditions.

Operating Cycles

An auditor divides the audit down into different cycles that make up the entire company. All related accounts within each cycle are audited together. Within each cycle, the auditor is concerned with what each specific employee does, the documents they handle and how each document relates to the segregation of ARCC'S (Authorization, Recording, Custody and Comparison). Controls have a function of either **Preventing** misstatements before they occur (most effective) or **Detecting and Correcting** misstatements that have already occurred (less expensive to implement, but could detect too late).

Revenue cycle (Sales Revenue / A.R./ Cash receipts)

The revenue cycle of a business consists of sales, billings, and collections. In order to properly segregate the incompatible functions of authorization, recording, and custody, the activities may include **specific employees** with each of the following duties (this list should be reviewed simply to make sure you are comfortable with the meaning of each job title):

- **Sales clerk** - Accepts orders from customers and prepares written sales orders (recording).
- **Credit manager** - Approves customer credit on orders (authorization).
- **Warehouse clerk** - Holds goods in inventory awaiting requests for shipment (custody).
- **Shipping clerk** - Removes items from inventory to ship to customer (custody).
- **Billing clerk** - Prepares sales invoices to send to customers (recording).
- **Receivables clerk** - *Posts* sales and collections to individual customer accounts based on sales invoices and remittance advices, respectively.
- **General ledger bookkeeper** - *Posts* journal entries for sales and collections.
- **Mail room clerk/receptionist** - Opens mail containing customer checks (or cash) and remittance advices, prepares a prelist (remittance listing) of checks, and directs these items to appropriate places (custody).