

ACC531: Auditing and Assurance Services  
Ch5. Internal Controls

Jaeyoon Yu, Ph.D.  
Central Michigan University

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls
- 5 Internal Control Evaluation
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication
- 7 Conclusion

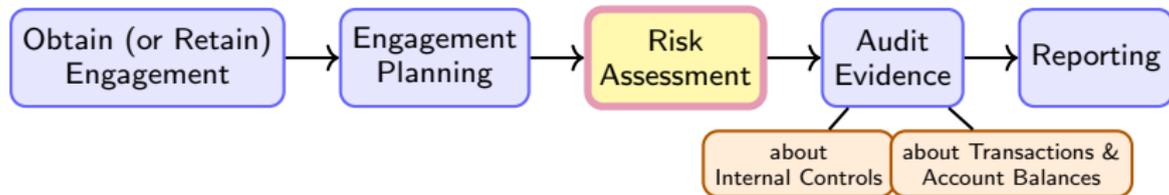
# Definition of Internal Control

---

## LO 5-1

Define and describe what is meant by internal controls.

- In Ch4, we introduced **Control Risk (CR)**: the probability that material misstatements will **not** be prevented or detected by the client's internal controls.
- To assess CR, auditors must first **understand** the client's internal control system.



# Motivating Example

---

**EX 1.** Suppose you run a retail store. You hire one employee to do all of:



**Q 1.** What could go wrong?

- Employee could steal cash from the register.
- Then alter records to conceal the theft.
- No one else would catch it — no \_\_\_\_\_<sup>1</sup>.

---

<sup>1</sup>An example of control activities.

## Definition: Internal Controls<sup>2</sup>

---

### Internal Controls (COSO, 2013)

A \_\_\_\_\_, effected by an entity's board of directors, management, and other personnel, designed to provide \_\_\_\_\_ regarding the achievement of objectives in:

- ① \_\_\_\_\_ — effectiveness and efficiency; safeguarding assets
- ② \_\_\_\_\_ — reliability of financial reporting
- ③ \_\_\_\_\_ — adherence to applicable laws and regulations

Auditors' primary focus is Internal controls over \_\_\_\_\_.

---

<sup>2</sup>Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control — Integrated Framework*, 2013.

# Three Key Elements of IC

---

## (1) A Process

Ongoing actions;  
not a one-time  
event

## (2) People

Board, MGT,  
and *all* personnel  
are involved

## (3) Reasonable Assurance

High confidence,  
not certainty

### Key Insight

ICs are designed & operated by people — inherently subject to human limitations.

## Reasonable Assurance

High level of confidence;  
attainable in practice

≠

## Absolute Assurance

100% certainty;  
unattainable in practice

Why can't IC provide **absolute** assurance?

- Cost-benefit constraint — eliminating all risk would be prohibitively expensive
- \_\_\_\_\_ — people make unintentional mistakes
- \_\_\_\_\_ — employees can cooperate to bypass controls
- \_\_\_\_\_ — authority can be used to circumvent controls

### Implication

These limitations are why auditors must **independently** assess IC, rather than simply accepting MGT's representations.

- ❶ Which of the following is **not** one of the three primary objectives of effective internal control? <sup>3</sup>
- A) Reliability of financial reporting
  - B) Efficiency and effectiveness of operations
  - C) Compliance with laws and regulations
  - D) Assurance of elimination of business risk
- ❷ Internal control is **not** designed to provide reasonable assurance that <sup>4</sup>
- A) All frauds will be detected
  - B) Transactions are executed in accordance with management's authorization
  - C) The company's resources are used efficiently and effectively
  - D) Company personnel comply with applicable rules and regulations

---

3

4

# Table of Contents

---

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls
- 5 Internal Control Evaluation
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication
- 7 Conclusion

## LO 5-2

Distinguish between the responsibilities of MGT and auditors regarding an entity's internal control.

## **MGT**

Responsible for  
designing, implementing,  
maintaining & assessing  
internal controls

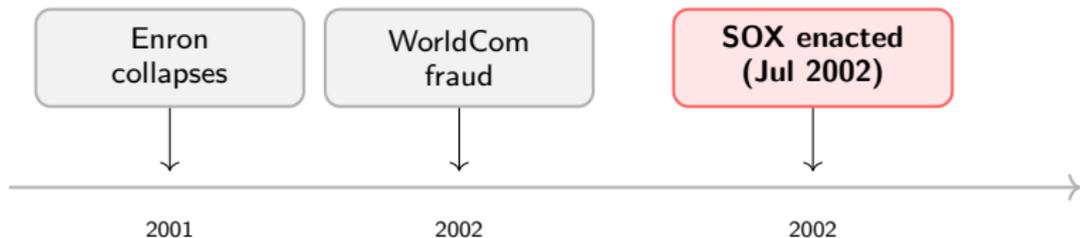
**vs.**

## **External Auditors**

Responsible for  
understanding & assessing  
internal controls

## Background: Why Does This Distinction Matter?

- Before 2002, there were no formal requirements for MGT to \_\_\_\_\_ or \_\_\_\_\_ IC.
- High-profile corporate frauds exposed the cost of weak MGT accountability.



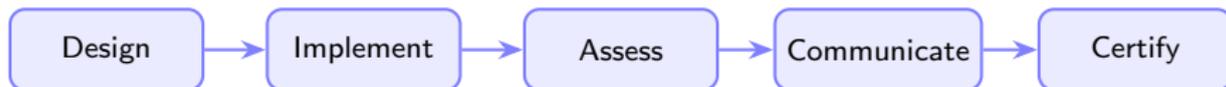
The Sarbanes-Oxley Act (SOX) formalized MGT's personal accountability for ICFR and required independent auditor \_\_\_\_\_.<sup>5</sup>

<sup>5</sup>Only for public companies.

# Management's Responsibilities

---

MGT is responsible for IC:



## SOX Section 302

CEOs and CFOs must personally certify in each 10-Q and 10-K filing that:

- They have \_\_\_\_\_ ICFR.<sup>a</sup>
- They have \_\_\_\_\_ any **MW** or **SD** to auditors and the audit committee.
- The FS are not **materially misleading**.

---

<sup>a</sup>ICFR: Internal Controls over Financial Reporting

---

<sup>6</sup>Included in the 10-K (annual) and 10-Q (quarterly) filings.

**ICFR**: Internal Controls over Financial Reporting;

**MW**: Material Weakness;

**SD**: Significant Deficiency

### SOX §404(a) — MGT's Annual Report on ICFR

In the *Form 10-K*, MGT must:

- 1 State **responsibility** for establishing and maintaining ICFR
- 2 Provide an **assessment** of ICFR effectiveness as of fiscal year-end
- 3 Identify the **framework** used (typically: \_\_\_\_\_)

#### Consequence of Weak ICFR

If one or more **MW** exist, MGT **must** conclude that ICFR is **ineffective**.

---

<sup>7</sup>Included in the 10-K (annual) filing.

**ICFR**: Internal Controls over Financial Reporting;

**MW**: Material Weakness;

**SD**: Significant Deficiency

## SOX §404(b) — External Auditor's Role

For **AFs**, the external auditor must:

- 1 **Independently** assess the design and operating effectiveness of ICFR
- 2 **Attest to and report on** MGT's assessment (not merely review it)
- 3 Issue a \_\_\_\_\_ on ICFR effectiveness

### Scope

Required for **AFs** under PCAOB AS 2201. **NAFs** (smaller public companies) are **exempt** from 404(b).

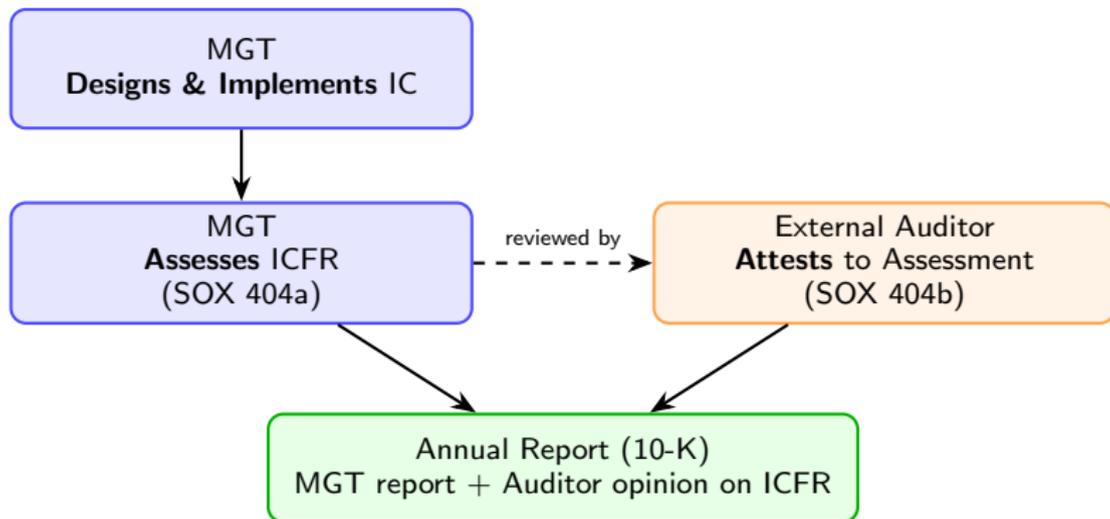
<sup>8</sup>Included in the 10-K (annual) filing.

**ICFR**: Internal Controls over Financial Reporting;

**AFs**: Accelerated Filers: Public firms with public float of \$75M+;

**NAFs**: Non-Accelerated Filers: Public firms with public float of less than \$75M;

**Public float**: market value of common stock held by non-affiliates. Conceptually, it's similar to market capitalization, but excludes stock held by insiders and large institutional investors.



Auditors must:<sup>9</sup>

- Obtain an understanding of ICFR relevant to the audit
- Evaluate the \_\_\_\_\_ of controls
- Test \_\_\_\_\_ effectiveness of controls
- Assess \_\_\_\_\_ risk and set planned detection risk accordingly
- For AFs: express an opinion on \_\_\_\_\_<sup>10</sup>

---

<sup>9</sup> [PCAOB AS 2201](#) (public) / [AU-C 315](#) (non-public).

<sup>10</sup> [AFs](#) (Accelerated Filers): Public firms with public float of \$75M+;

## Practice: Responsibilities for Internal Control

---

- 1 When one material weakness is present at year-end, management of a public company must conclude that ICFR is<sup>11</sup>
- A) Insufficient
  - B) Inadequate
  - C) Ineffective
  - D) Inefficient
- 2 [T/F] SOX requires **both** management **and** auditors to report on ICFR effectiveness.<sup>12</sup>
- 3 [T/F] Only larger public companies (accelerated filers) are required to obtain an auditor report on ICFR.<sup>13</sup>
- 4 [T/F] Two key concepts for designing IC are *absolute assurance* and *inherent limitations*.<sup>14</sup>

---

11

12

13

14

# Table of Contents

---

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control**
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls
- 5 Internal Control Evaluation
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication
- 7 Conclusion

## LO 5-3

Describe the five basic components of internal control.  
Specify some of their characteristics.

## Overview: Five Components (COSO 2013)

---



All five components must be present and functioning for internal control to be effective.

## Control Environment

The **foundation** for all other components; sets the organizational **tone, culture, and structure** within which IC operates. Often called the **“tone at the top.”**

Key elements:

- Commitment to \_\_\_\_\_ and ethical values
- Board of directors' \_\_\_\_\_ and oversight
- Clear organizational structure and assignment of authority
- Commitment to recruit and retain competent personnel
- \_\_\_\_\_ for performance

### Key Point

The control environment has a **pervasive effect** on all other components — a weak foundation undermines everything built on top of it.

## Enron (2001):

- Board approved conflicting-interest transactions without scrutiny
- CFO had authority to \_\_\_\_\_ financial reporting controls
- Written code of conduct existed — culture did not enforce it

## WorldCom (2002):

- CEO pressured staff to “make the numbers”
- Internal audit lacked \_\_\_\_\_ from MGT
- \$11B in operating expenses improperly \_\_\_\_\_

### Lesson

SOX was enacted largely in response to **control environment failures** — not failures of specific control activities.

## Risk Assessment

A dynamic and iterative process for identifying and analyzing risks to achieving objectives, forming the basis for determining how risks should be managed.

- Firms need to manage the full range of business risks including reporting risks.
- MGT must \_\_\_\_\_ and analyze risks to the objectives.
- MGT must \_\_\_\_\_ and \_\_\_\_\_ to the risks.
- Although a client's risk assessment process should relate to all its objectives, auditing standards require that the audit team focus on financial reporting risks including fraud risk.

## Control Activities

The actions and procedures that help ensure MGT's risk-mitigation directives are carried out.

Three types of control activities:<sup>15</sup>

- \_\_\_\_\_ controls - stop errors before they occur
- \_\_\_\_\_ controls - catch errors after the fact
- \_\_\_\_\_ controls - correct errors after the fact

---

<sup>15</sup>In some sense, all IC activities might be understood as “preventive” as they help to prevent errors before they occur.

- **Management review controls** — MGT is primary responsible for the IC process, so it is important to review the IC process to ensure it is effective.
- **Information processing controls** — ensure that the information is processed correctly and efficiently.
  - ▶ **Automated controls** — use technology to control the process.
  - ▶ **Manual controls** — use manual processes to control the process.
- **Physical security controls** — safeguard assets, data, documents, and records, etc.
- **Separation of duties** — ensure that no one person has control over all aspects of a process.

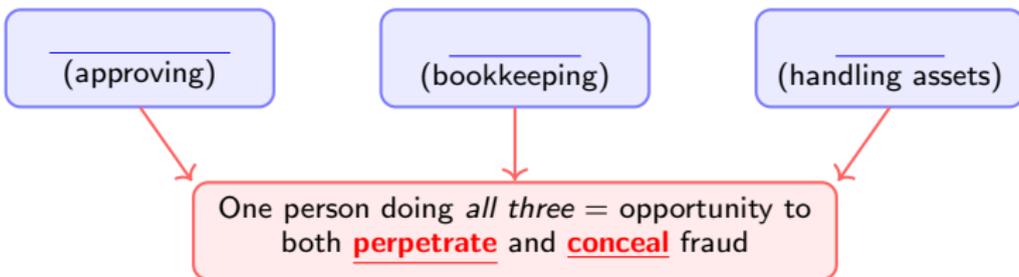
---

<sup>16</sup>Organizations have a wide range of control activities, and the following are just a few examples.

# Control Activities: Segregation of Duties

---

Three **incompatible** functions should be kept **separate**:



## Information & Communication

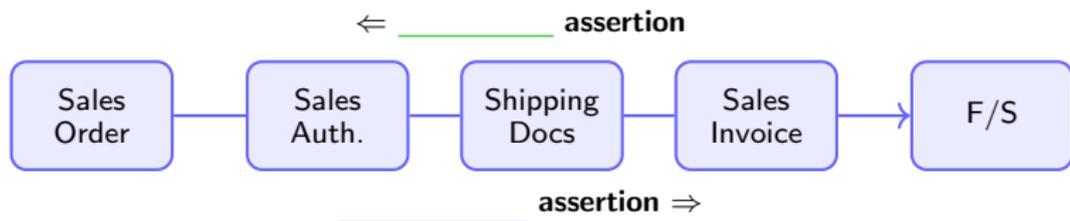
MGT obtains or generates relevant, quality information to support IC, and communicates it internally and externally.

- MGT must have access to timely, reliable, and relevant information.
- MGT must generate relevant, quality information to support IC.
- MGT must communicate the information internally and externally.

Information system produces a trail of activities (a.k.a. audit trail) from data identification to financial reports.

- From the source documents (purchase orders, sales orders, etc.)
- To the financial reports.

Auditors often follow this trail forward and backward to assess management assertions:



## Monitoring Activities

Ongoing and/or separate evaluations used to ascertain whether each component of IC is **present and functioning**, with deficiencies communicated timely.

- **Ongoing and separate evaluations**: Ongoing evaluations of controls that are separate from other types of evaluations enable MGT to determine whether the other components of IC continue to function over time.
- **Reporting deficiencies**: IC deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action and MGT and BOD as appropriate.

**Effective monitoring** involves ongoing evaluation of controls:

- **Periodic evaluation of controls** by the internal audit department.
- Analysis of and appropriate **follow-up** of operating reports or metrics that might identify anomalies indicative of a control failure.
- **Supervisory review of controls**, such as reconciliation reviews as a normal part of processing.
- **Self-assessment** by BOD and MGT regarding the tone they set in the organization and the effectiveness of their oversight functions.
- **Audit committee inquiries** of internal and external auditors.
- **Quality assurance reviews** of the internal audit department.

### 1 Control Environment

- 1 The organization demonstrates a commitment to **integrity** and **ethical values**.
- 2 The BOD demonstrates **independence** from MGT and exercises oversight of the development and performance of IC.
- 3 MGT, with board oversight, establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- 4 The organization demonstrates a commitment to attract, develop, and retain **competent** individuals in alignment with objectives.
- 5 The organization holds individuals **accountable** for their IC responsibilities.

### 2 Risk Assessment

- 1 The organization specifies **objectives** with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- 2 The organization identifies and analyzes **risks** to the achievement of its objectives.
- 3 The organization considers the potential for **fraud** in assessing risks to the achievement of objectives.
- 4 The organization identifies and assesses **changes** that could significantly impact the system of internal control.

### 3 Control Activities

- 1 The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- 2 The organization selects and develops general controls over technology to support the achievement of objectives.
- 3 The organization deploys control activities through policies and procedures.

### 4 Information and Communication

- 1 The organization obtains or generates and uses relevant, quality information to support the functioning of IC.
- 2 The organization internally communicates information, including objectives and responsibilities for IC, necessary to support the functioning of IC.
- 3 The organization communicates with external parties regarding matters affecting the functioning of IC.

### 5 Monitoring Activities

- 1 The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of IC are present and functioning.
- 2 The organization evaluates and communicates IC deficiencies in a timely manner to those parties responsible for taking corrective action.

- 1 Without an effective \_\_\_\_\_, the other COSO components are unlikely to result in effective IC, regardless of their quality.<sup>17</sup>
- A) Risk assessment policy
  - B) Monitoring policy
  - C) Control environment
  - D) System of control activities
- 2 Proper segregation of functional responsibilities calls for separation of<sup>18</sup>
- A) Authorization, execution, and payment
  - B) Authorization, recording, and custody
  - C) Custody, execution, and reporting
  - D) Authorization, payment, and recording

---

17

18

# Table of Contents

---

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls**
- 5 Internal Control Evaluation
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication
- 7 Conclusion

Modern accounting systems are **IT-based**: transactions are initiated, processed, and stored electronically.

### Key risks introduced by IT:

- **Systematic errors** — one programming error affects *all* transactions processed
- **Unauthorized access** — centralized data accessible remotely
- **Collapsed duties** — IT systems may perform authorization *and* recordkeeping automatically, violating \_\_\_\_\_

Two types of IT controls:

- \_\_\_\_\_ controls — apply to the entire IT environment
- \_\_\_\_\_ controls — apply to a specific software application

### General Controls

Controls that relate to the overall IT environment and have a pervasive effect on all software applications.

---

Category	Examples
Administration	IT steering committee; IT policies and procedures
Segregation of IT Duties	Systems development   Computer operations   Data control
Systems Development	Testing and user approval of new/changed programs
Physical & Online Security	Locked computer rooms; key-card access; passwords; firewalls
Backup & Contingency	Off-site backup copies; disaster recovery plan
Hardware Controls	Parity checks; echo checks; error detection

---

### Application Controls

Controls that apply to the processing of individual transaction types within a specific software application.

#### Input Controls

Verify data entry:  
valid employee ID;  
field format checks;  
batch totals

#### Processing Controls

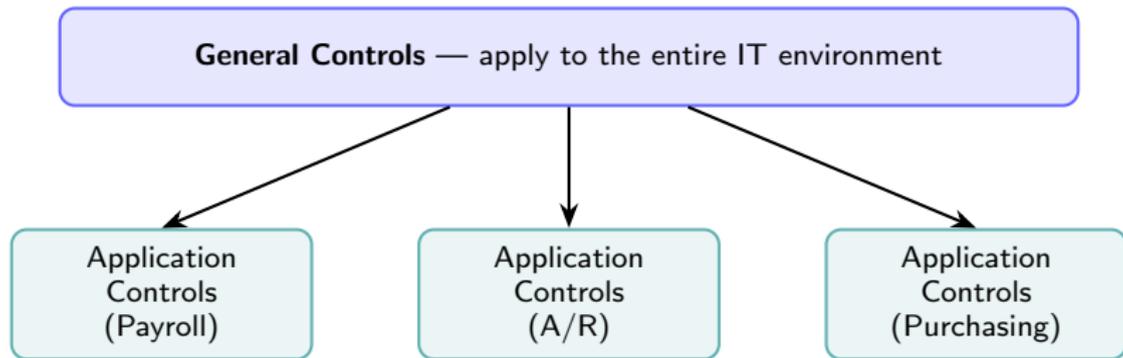
Ensure complete  
and accurate  
processing:  
sequence checks;  
run-to-run totals

#### Output Controls

Verify outputs  
are complete and  
sent to authorized  
recipients only

**Example:** A payroll application that rejects time records with employee IDs not in the HR database is an input control.

## Appendix: General Controls vs. Application Controls



### Critical Rule

If **general controls are weak**, application controls **cannot be relied upon** — regardless of their apparent design quality. Auditors test \_\_\_\_\_ controls first.

- 1 General controls include all of the following **except**<sup>19</sup>
- A) Systems development
  - B) Online security
  - C) Processing controls
  - D) Hardware controls
- 2 Which best explains the relationship between general controls and application controls?<sup>20</sup>
- A) Application controls are effective even if general controls are extremely weak.
  - B) Application controls are likely to be effective only when general controls are effective.
  - C) General controls have no impact on application controls.
  - D) None of the above.

---

19

20

# Table of Contents

---

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls
- 5 Internal Control Evaluation**
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication
- 7 Conclusion

### LO 5-4

Explain the process the audit team uses to assess control risk. Understand its impact on the RMM and how it affects the nature, timing, and extent of further audit procedures.

## Step 1: Obtain an Understanding of IC

---

Before assessing risk, auditors must **obtain and document** an understanding of all five COSO components:



## Step 1: Obtain an Understanding of IC

---

Auditors mainly use four methods to obtain an understanding of IC:

- **Narratives** — written descriptions of the client's IC.
- **Questionnaires** — standardized checklists of IC questions.
- **Flowcharts** — visual diagrams of the flow of transactions through the accounting system.
- **Walk-through** — tracing a transaction from initiation through recording to reporting.



- 1 Narratives, flowcharts, and IC questionnaires are three common methods of<sup>22</sup>
  - A) Testing IC
  - B) Documenting the auditor's understanding of IC
  - C) Designing audit procedures
  - D) Documenting organizational structure
  
- 2 [T/F] Walkthroughs combine observation, inspection, and inquiry to confirm that controls designed by management have been implemented.<sup>23</sup>
  
- 3 [T/F] Auditors are required to use narratives when documenting their understanding of IC.<sup>24</sup>
  
- 4 [T/F] When using questionnaires, “no” responses typically indicate a potential IC deficiency requiring follow-up.<sup>25</sup>

---

22

23

24

25

### Control Risk (CR)

The probability that material misstatements will not be prevented or detected by the client's internal controls.

- Auditors assess **how well** controls prevent or detect misstatements.
- The assessment is important for auditors to decide whether to rely on \_\_\_\_\_ or perform \_\_\_\_\_.
- The assessment directly affects the **nature, timing, and extent (NTE)** of further procedures.

## Control Risk Assessed as **HIGH**

---

- Controls are \_\_\_\_\_ at preventing or detecting misstatements.
- Audit team \_\_\_\_\_ rely on controls.

### Audit response (N/T/E):

- **Nature:** more substantive \_\_\_\_\_ (vouching, confirmations).
- **Timing:** testing near year-end (closer to balance sheet date).
- **Extent:** \_\_\_\_\_ sample sizes and \_\_\_\_\_ procedures.

- Controls are \_\_\_\_\_ at preventing or detecting misstatements.
- Audit team can \_\_\_\_\_ on controls.

### **Audit response (N/T/E):**

- **Nature:** more analytical \_\_\_\_\_ (relative to tests of details).
- **Timing:** testing at an **interim date** (before fiscal year-end).
- **Extent:** \_\_\_\_\_ sample sizes and \_\_\_\_\_ procedures.

## Control Risk Assessment: Summary

---

	<b>CR High</b>	<b>CR Low</b>
Controls effective?	No — cannot be relied upon	Yes — can be relied upon
Nature	Substantive tests of details	More analytical procedures
Timing	Near year-end	Interim date
Extent	Large sample sizes	Smaller sample sizes

The **control risk matrix** links specific controls to audit objectives, helping auditors identify where CR is low or high.

Audit Objective	Control A	Control B	Assessed CR
Occurrence	✓		<u>Low</u>
Completeness		✓	<u>Low</u>
Accuracy	✓	✓	<u>Low</u>
Cut-off			<u>High</u>

- **Entity-level controls** (e.g., strong audit committee) can reduce CR across many objectives
- Objectives with **no applicable controls** = maximum CR ⇒ more substantive testing required
- A **compensating control** elsewhere may offset the absence of a primary control

## Control Deficiency Types<sup>26</sup>

When assessing CR, auditors classify any problems found:

Type	Definition
<b>CD</b>	A control is missing or not operating effectively.
<b>SD</b>	Less severe than a material weakness, but <b>important enough</b> to merit attention by those charged with governance.
<b>MW</b>	Reasonable possibility that a <b>material misstatement</b> will not be <b>prevented or detected</b> on a timely basis.



If there is one or more MW, the ICFR is **ineffective**.

<sup>26</sup> **CD**: Control Deficiency;  
**SD**: Significant Deficiency;  
**MW**: Material Weakness

- 1 Which deficiency exists if a necessary control is **missing** or not properly implemented?<sup>27</sup>
- A) Control deficiency
  - B) Significant deficiency
  - C) Design deficiency
  - D) Operating deficiency
- 2 A \_\_\_\_\_ exists if one or more control deficiencies are less severe than a material weakness, but important enough to merit attention by those charged with governance.<sup>28</sup>
- A) Potential misstatement
  - B) Significant weakness
  - C) Significant deficiency
  - D) Fraud symptom

---

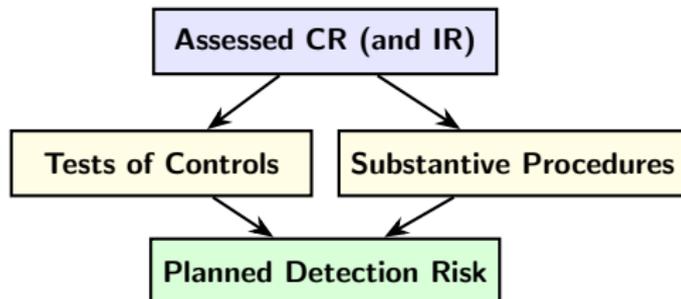
27

28

# Control Risk and Audit Planning

Recall:  $AR = IR \times CR \times DR$ . Solving for DR:

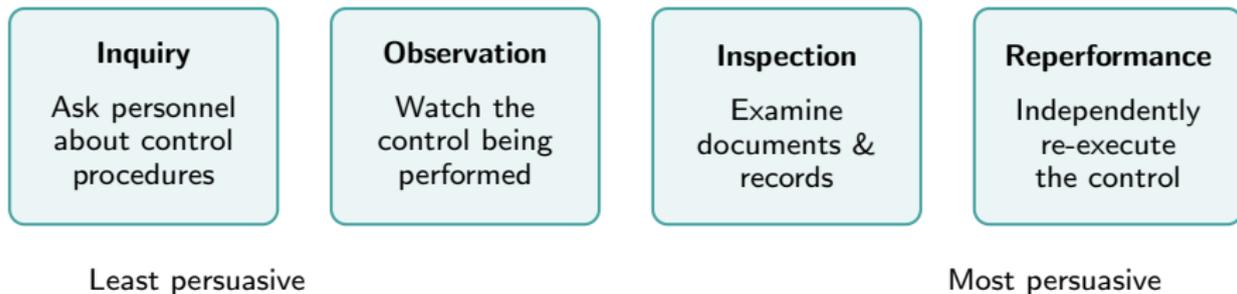
- **Higher CR**  $\Rightarrow$  lower allowable \_\_\_  $\Rightarrow$  more \_\_\_\_\_
- **Lower CR**  $\Rightarrow$  higher allowable \_\_\_  $\Rightarrow$  less \_\_\_\_\_



### Tests of Controls

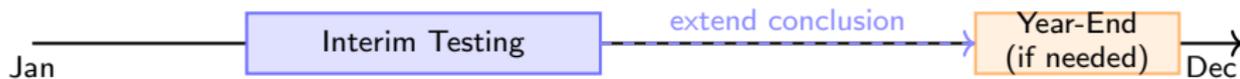
Audit procedures designed to evaluate the operating effectiveness of controls in preventing or detecting material misstatements at the assertion level.

- Auditors perform tests of controls when they plan to rely on controls to reduce substantive testing.
- Indeed, auditors would like to reduce substantive testing by relying on controls while maintaining acceptable audit risk.



- **Inquiry alone** is insufficient — auditors must **corroborate** with observation, inspection, or re-performance.
- **Observation** — Employees may perform the control differently under being observed.
- **Reperformance** — Auditors directly perform the control to assess its effectiveness.

# Timing and Extent of Tests of Controls



- **Timing:** \_\_\_\_\_ common  
→ extend conclusion to year-end with limited additional work
- **Manual vs. Automated:**
  - ▶ \_\_\_\_\_ controls: consistent ⇒ prior-year reliance possible<sup>29</sup>
  - ▶ \_\_\_\_\_ controls: variable ⇒ more frequent testing required<sup>30</sup>

<sup>29</sup> assuming no changes to the control; still should be tested every three years under Auditing Standards.

<sup>30</sup> likely to include human error; so should be tested every year.

## Tests of Controls vs. Substantive Procedures

	Tests of Controls	Substantive Procedures
<b>Purpose</b>	Evaluate whether IC is <u>operating</u> effectively	Detect <u>material misstatements</u> in account balances / transactions
<b>Target</b>	Controls (policies, procedures)	Financial statement assertions
<b>When used</b>	When auditor plans to <u>rely</u> on controls	<u>Always</u> performed (extent varies with CR)
<b>Result</b>	Supports assessed CR	Direct evidence on FS amounts

Once again, the goal of tests of controls is to evaluate the \_\_\_\_\_ of controls in preventing or detecting material misstatements at the assertion level.

If not effective, auditors will \_\_\_\_\_ the extent of substantive procedures to compensate.

In the end, the ultimate goal is to maintain the desired level of \_\_\_\_\_ risk.

- 1 Tests of controls are<sup>31</sup>
  - A) Procedures used to test the effectiveness of controls in support of a reduced assessed control risk
  - B) Used to support ending balances in the balance sheet and income statement accounts
  - C) Performed only at the end of the audit
  - D) Designed to detect fraud
  
- 2 [T/F] Controls applied throughout the period must be tested at **both** an interim date and again on the balance sheet date.<sup>32</sup>
  
- 3 [T/F] Auditing standards require auditors to test some prior-year controls each year to ensure rotation throughout a three-year period.<sup>33</sup>

---

31

32

33

# Table of Contents

---

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls
- 5 Internal Control Evaluation
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication**
- 7 Conclusion

## LO 5-5

Explain the communication of internal control deficiencies to those charged with governance such as audit committee and other key MGT personnel.

### Deficiency

A deficiency exists when a control does **not** allow MGT/employees to prevent or detect misstatements timely. Two root causes:

- **Design deficiency** — control is **missing** or poorly conceived
  - **Operating deficiency** — control is designed well but **not functioning** as intended
- 
- If a deficiency, or a combination of deficiencies, results in a reasonable possibility that a MM will not be prevented or detected on a timely basis, it is a \_\_\_\_.
  - If a deficiency, or a combination of deficiencies in IC is less severe than a **MW**, it is a \_\_\_\_.
  - Audit team must communicate both SD and MW to the MGT, BOD, and AC in writing.<sup>34</sup>

<sup>34</sup> MGT: Management; BOD: Board of Directors; AC: Audit Committee

<sup>35</sup> **MW**: Material Weakness; **SD**: Significant Deficiency

# Types of Opinions on ICFR (Integrated Audit)

Opinion Type	Condition
Effective	No MWs
Ineffective	1+ MWs exist
No Conclusion	Scope limitation <sup>36</sup>

## Implications of Adverse Opinion on ICFR

An **adverse opinion (i.e., ineffective)** on ICFR does **not** automatically mean that the FS includes MM. It only means higher likelihood of MM.

<sup>36</sup>cannot obtain sufficient evidence

# Table of Contents

---

- 1 Definition of Internal Control
- 2 MGT vs. Auditors' Responsibility for Internal Control
- 3 Components of Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring
- 4 Appendix: IT Controls
- 5 Internal Control Evaluation
  - Understand and Document IC
  - Assess Control Risk
  - Tests of Controls
- 6 Internal Control Communication
- 7 Conclusion

**Internal controls** should be:

- \_\_\_\_\_ properly to prevent and detect MM and
- \_\_\_\_\_ effectively as intended.

**Effective internal controls** would:

- \_\_\_\_\_ the need for substantive testing.

**Reporting: Opinions on ICFR:**

- Public firms with public float of \$75M+: required by \_\_\_\_\_
- Other public firms and all private firms: exempt.
- Still, auditors must communicate any SD and MW to those charged with governance in writing — usually MGT, BOD, and AC.

# Classification of Control Activities

---

We covered various control activities in the previous slides. It is important to organize them into a systematic way.

By the degree of scope:

- 1 Entity-level controls — apply to the entire entity.
- 2 Transaction-level controls

By functions:

- 1 Preventive controls
- 2 Detective controls
- 3 Corrective controls

By locations for controls:

- 1 Physical controls
- 2 IT general controls (ITGCs) — apply to the entire IT environment.
- 3 IT application controls

By the degree of automation:

- 1 Purely manual controls
- 2 Manual controls with system-generated reports
- 3 Automated controls