ACC531: Auditing and Assurance Services

Ch5. Internal Controls

Jaeyoon Yu, Ph.D.
Central Michigan University

Table of Contents

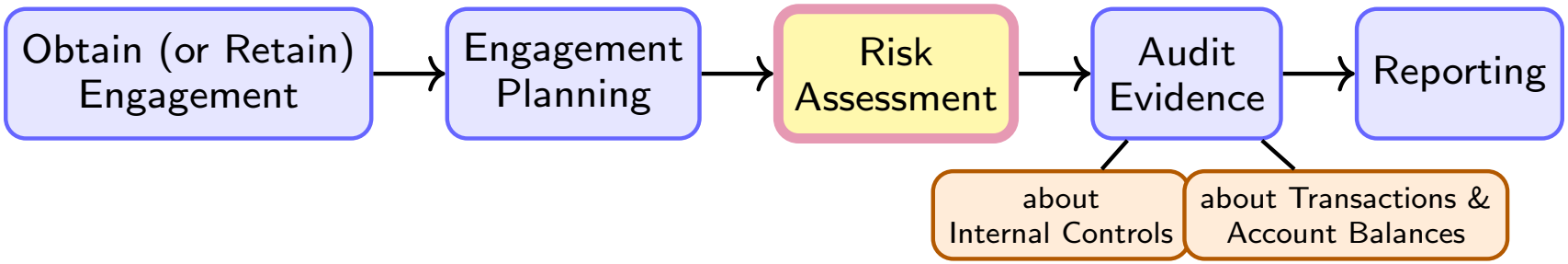
Definition of Internal Control

LO 5-1

Define and describe what is meant by internal controls.

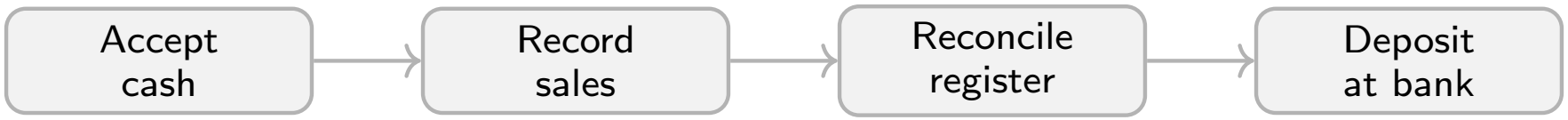
Where Are We?

- 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 **segregation of duties**.[1]

[1] An example of control activities.

Definition: Internal Controls[2]

Internal Controls (COSO, 2013)

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

1. **Operations** — effectiveness and efficiency; safeguarding assets
2. **Reporting** — reliability of financial reporting
3. **Compliance** — adherence to applicable laws and regulations

Auditors' primary focus is Internal controls over **financial reporting (ICOFR)**.

[2] 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.

Inherent Limitations of IC

Reasonable Assurance

High level of confidence; attainable in practice

$\neq$

Absolute Assurance

100% certainty; unattainable in practice

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

- Cost-benefit constraint — eliminating all risk would be prohibitively expensive
- **Human error** — people make unintentional mistakes
- **Collusion** — employees can cooperate to bypass controls
- **MGT override** — authority can be used to circumvent controls

Implication

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

Practice: Definition of Internal Control

1. Which of the following is **not** one of the three primary objectives of effective internal control? [3]
   - **A)** Reliability of financial reporting
   - **B)** Efficiency and effectiveness of operations
   - **C)** Compliance with laws and regulations
   - **D)** Assurance of elimination of business risk

2. Internal control is **not** designed to provide reasonable assurance that [4]
   - **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] **D**
[4] **A**

Table of Contents

MGT vs. Auditors' Responsibility for Internal Control

LO 5-2

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

The Core Distinction

MGT

Responsible for

designing, implementing, maintaining & assessing internal controls

vs.

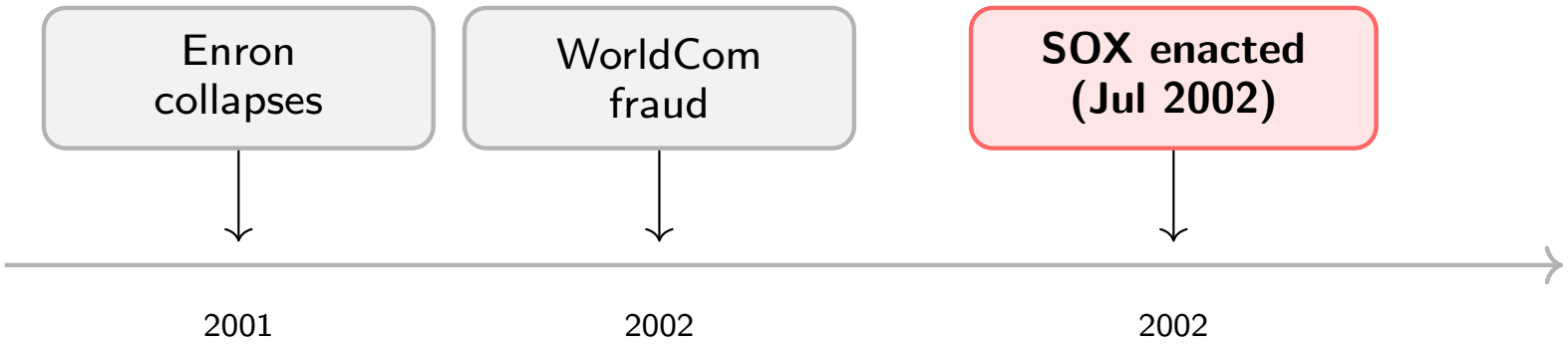
External Auditors

Responsible for

understanding & assessing internal controls

Background: Why Does This Distinction Matter?

- Before 2002, there were no formal requirements for MGT to **certify** or **assess** 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** **attestation**.[5]

[5] Only for public companies.

Management's Responsibilities

MGT is **responsible for** IC:

SOX §302: CEO/CFO Certification[6]

SOX Section 302

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

- They have **reviewed** ICFR.[a]
- They have **disclosed** any **MW** or **SD** to auditors and the audit committee.
- The FS are not **materially misleading**.

[a] ICFR: Internal Controls over Financial Reporting

[6] 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): Management Assessment[7]

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: **COSO**)

Consequence of Weak ICFR

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

[7] Included in the 10-K (annual) filing.
ICFR: Internal Controls over Financial Reporting;
MW: Material Weakness;
SD: Significant Deficiency

SOX §404(b): Auditor Attestation[8]

SOX §404(b) — External Auditor's Role

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

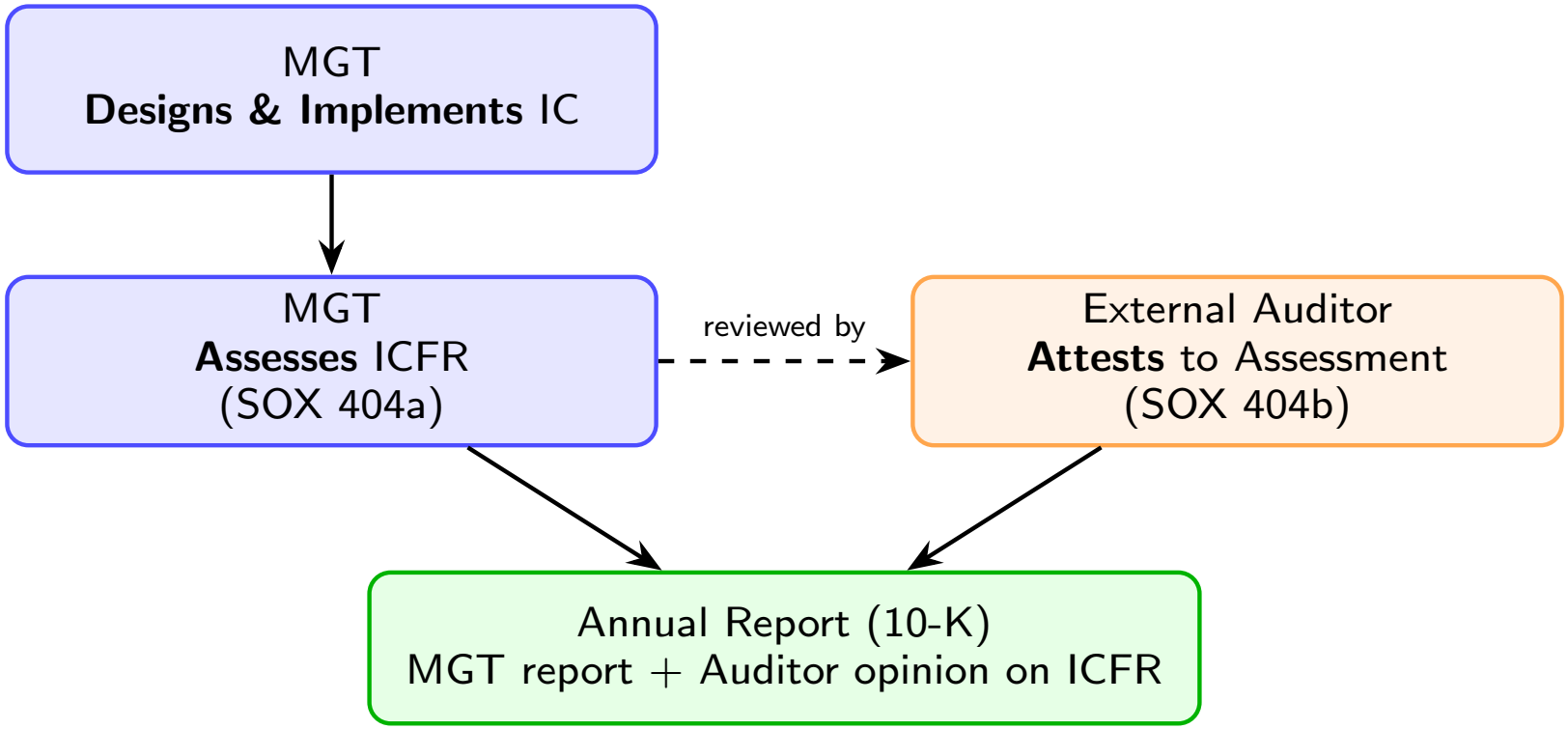
1. **Independently** assess the design and operating effectiveness of ICFR
2. **Attest to and report on** MGT's assessment (not merely review it)
3. Issue a **separate opinion** on ICFR effectiveness

Scope

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

[8] 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.

SOX 404: Process Flow



Auditors' Responsibilities

Auditors must:[9]

- Obtain an understanding of ICFR relevant to the audit
- Evaluate the **design** of controls
- Test **operating** effectiveness of controls
- Assess **control** risk and set planned detection risk accordingly
- For AFs: express an opinion on **ICFR**[10]

[9] **PCAOB AS 2201** (public) / **AU-C 315** (non-public).
[10] **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[11]
   - **A)** Insufficient
   - **B)** Inadequate
   - **C)** Ineffective
   - **D)** Inefficient

2. [T/F] SOX requires **both** management **and** auditors to report on ICFR effectiveness.[12]

3. [T/F] Only larger public companies (accelerated filers) are required to obtain an auditor report on ICFR.[13]

4. [T/F] Two key concepts for designing IC are *absolute assurance* and *inherent limitations*.[14]

[11] **C**
[12] **F**
[13] **T**
[14] **F**

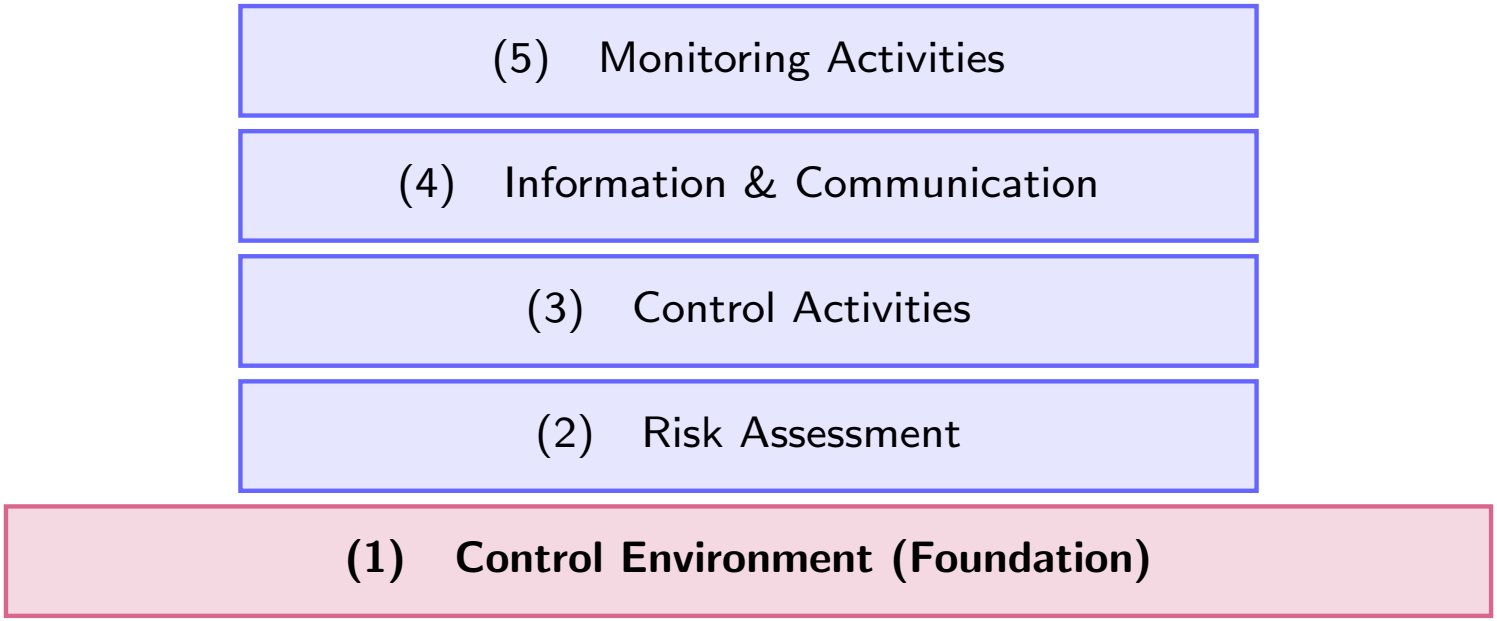
Table of Contents

Components of Internal Control

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 **integrity** and ethical values
- Board of directors' **independence** and oversight
- Clear organizational structure and assignment of authority
- Commitment to recruit and retain competent personnel
- **Accountability** 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.

Control Environment: Real-World Failures

Enron (2001):

- Board approved conflicting-interest transactions without scrutiny
- CFO had authority to **bypass** 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 **independence** from MGT
- $11B in operating expenses improperly **capitalized**

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 **identify** and analyze risks to the objectives.
- MGT must **assess** and **respond** 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:[15]

- **Preventive** controls - stop errors before they occur
- **Detective** controls - catch errors after the fact
- **Corrective** controls - correct errors after the fact

[15] In some sense, all IC activities might be understood as "preventive" as they help to prevent errors before they occur.

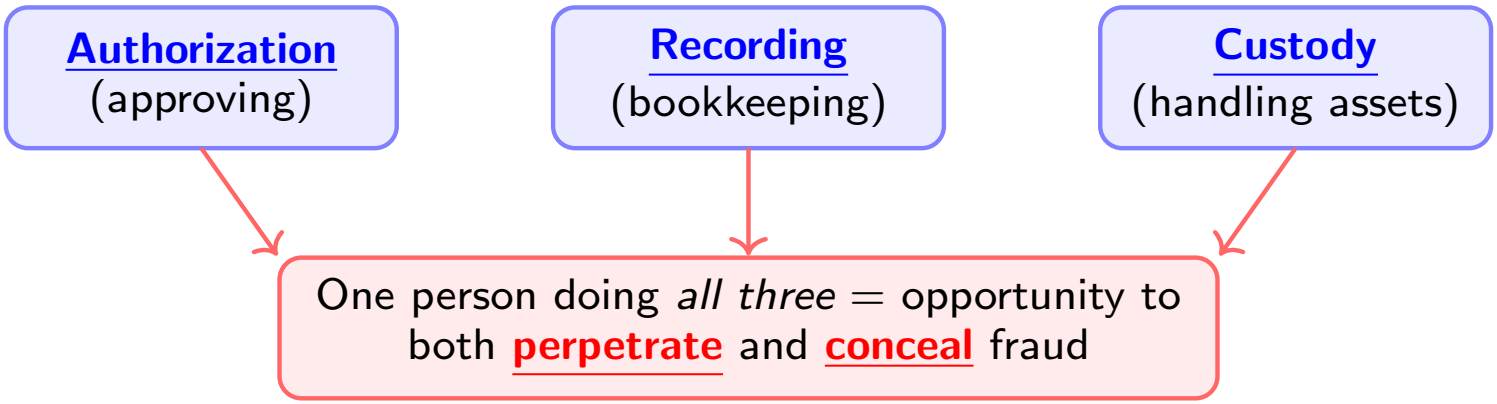
Examples of Control Activities[16]

- **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.

[16] Organizeations 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**.

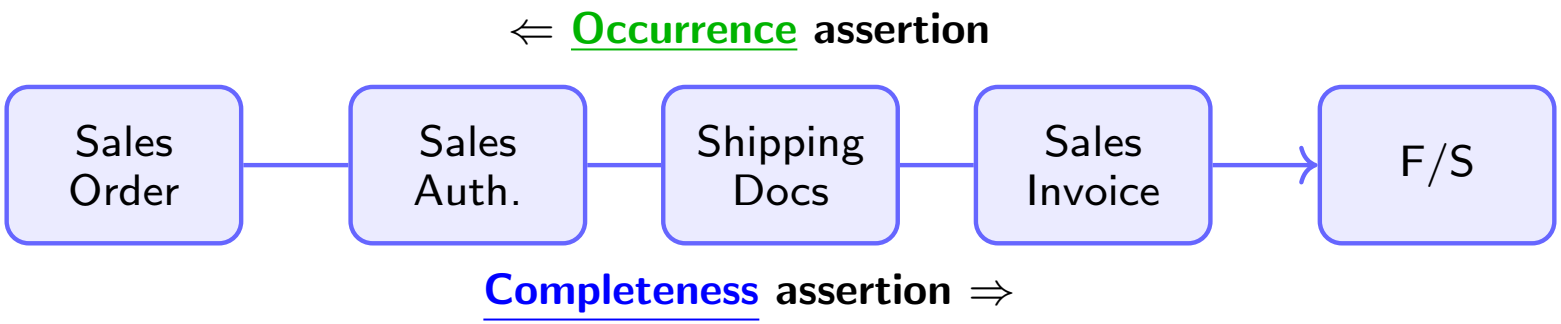
- MGT must have access to timely, reliable, and relevant information.
- MGT must generate relevant, quality information to support IC.
- MGT must communicate the information internally and externally.

Information and Communication

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 fronward and backward to assess management assertions:



Monitoring

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.

Monitoring

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 orgnization and the effectiveness of their oversight functions.
- **Audit committee inquiries** of internal and external auditors.
- **Quality assurance reviews** of the internal audit department.

Summary: The 17 COSO 2013 Principles (1 of 2)

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.

Summary: The 17 COSO 2013 Principles (2 of 2)

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.

Practice: COSO Framework

1. Without an effective _____, the other COSO components are unlikely to result in effective IC, regardless of their quality.[17]
   - **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[18]
   - **A)** Authorization, execution, and payment
   - **B)** Authorization, recording, and custody
   - **C)** Custody, execution, and reporting
   - **D)** Authorization, payment, and recording

[17] **C**
[18] **B**

Table of Contents

Appendix: Why IT Controls Matter

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 **separation of duties**

Two types of IT controls:

- **General** controls — apply to the entire IT environment
- **Application** controls — apply to a specific software application

Appendix: IT General Controls

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

Appendix: IT Application Controls

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

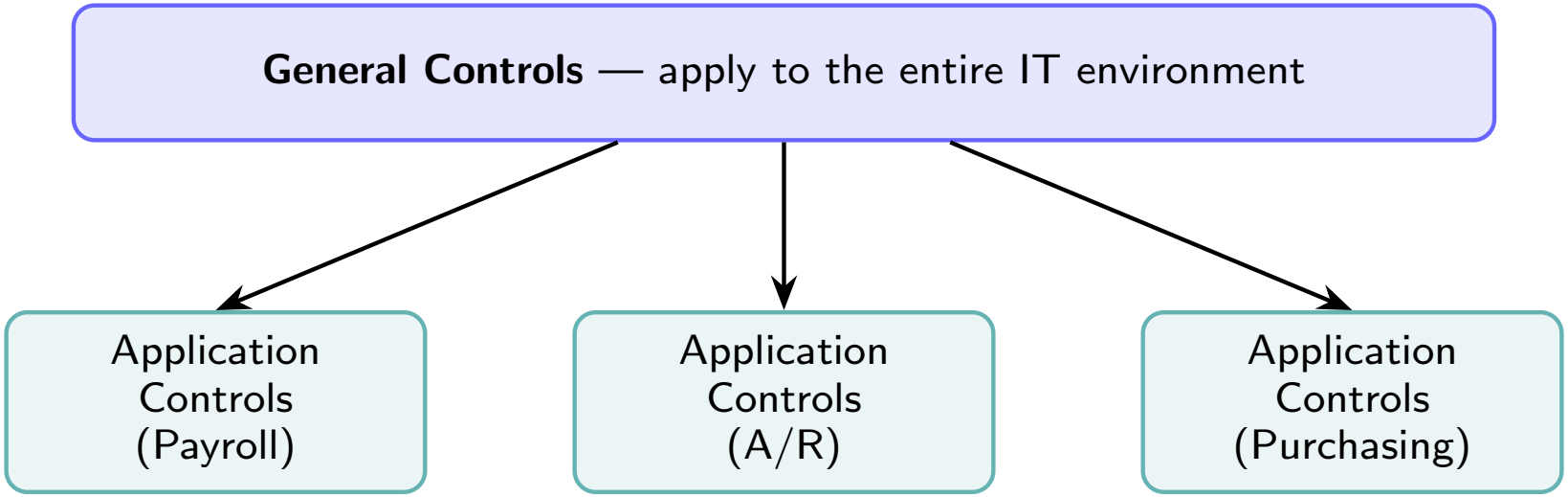
Ensure complete and accurate processing: sequence checks; run-to-run totals

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 **general** controls first.

Practice: IT Controls

1. General controls include all of the following **except**[19]
   - **A)** Systems development
   - **B)** Online security
   - **C)** Processing controls
   - **D)** Hardware controls

2. Which best explains the relationship between general controls and application controls?[20]
   - **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] **C**
[20] **B**

Table of Contents

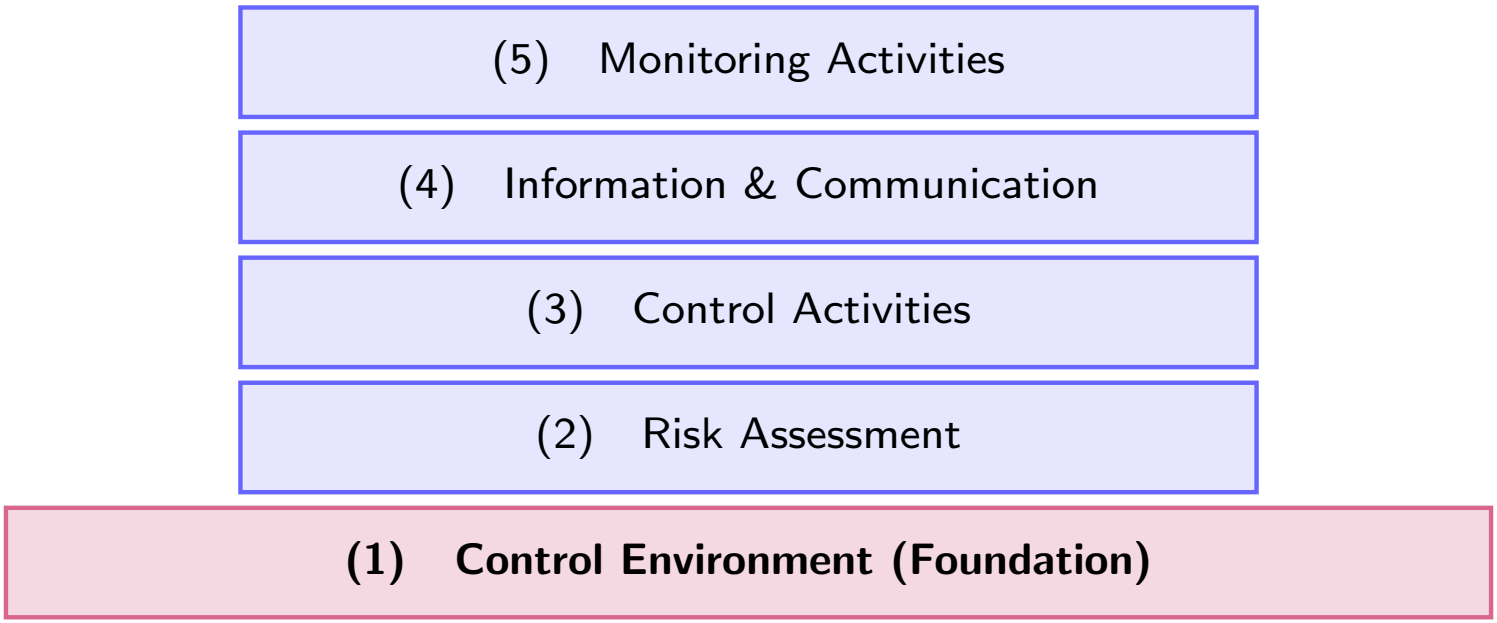
Internal Control Evaluation

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

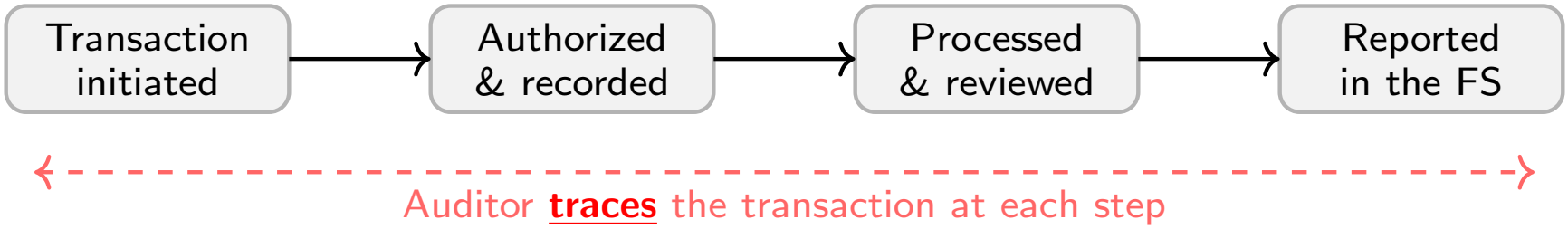
Auditors mainly use four methods to obtain an understanding of IC:

- **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.

Step 1: Obtain an Understanding of IC — Walk-Through

Walk-Through

Tracing **one or a few transactions** through the entire information system — from initiation to recording in the FS — to confirm the auditor's understanding of IC.



Walk-thorough usually includes four methods used to perform Tests of Controls later:[21]

1. **Inquiry**
2. **Observation**
3. **Inspection**
4. **Re-performance**

[21] Here we're in Step 1: Understanding and Documenting IC. These methods will be used in Step 3: Tests of Controls much more extensively.

Practice: Understanding and Documenting IC

1. Narratives, flowcharts, and IC questionnaires are three common methods of[22]
   - **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.[23]

3. [T/F] Auditors are required to use narratives when documenting their understanding of IC.[24]

4. [T/F] When using questionnaires, "no" responses typically indicate a potential IC deficiency requiring follow-up.[25]

---

[22] **B**
[23] **T**
[24] **F**
[25] **T**

Step 2: Assess Control Risk

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 **controls** or perform **substantive procedures**.
- The assessment directly affects the **nature, timing, and extent (NTE)** of further procedures.

Control Risk Assessed as **HIGH**

- Controls are **not effective** at preventing or detecting misstatements.
- Audit team **can't** relyon controls.

Audit response (N/T/E):

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

Control Risk Assessed as **LOW**

- Controls are **effective** at preventing or detecting misstatements.
- Audit team can **rely** on controls.

Audit response (N/T/E):

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

Control Risk Assessment: Summary

	CR High	**CR Low**
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

Control Risk Matrix

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

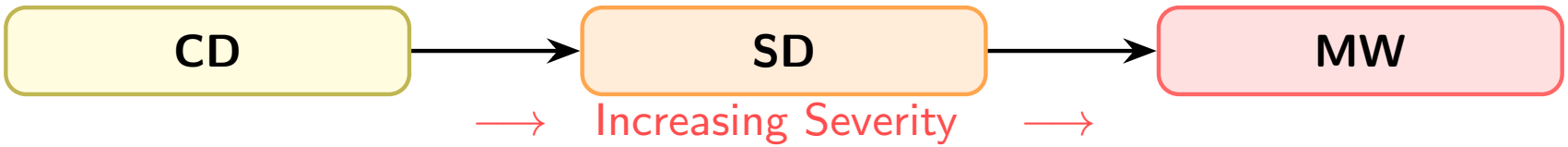
Audit Objective	Control A	Control B	Assessed CR
Occurrence	✓		**Low**
Completeness		✓	**Low**
Accuracy	✓	✓	**Low**
Cut-off			**High**

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

Control Deficiency Types[26]

When assessing CR, auditors classify any problems found:

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



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

[26] **CD**: Control Deficiency;
SD: Significant Deficiency;
MW: Material Weakness

Practice: Control Risk Assessment

1. Which deficiency exists if a necessary control is **missing** or not properly implemented?[27]
   - **A)** Control deficiency
   - **B)** Significant deficiency
   - **C)** Design deficiency
   - **D)** Operating deficiency

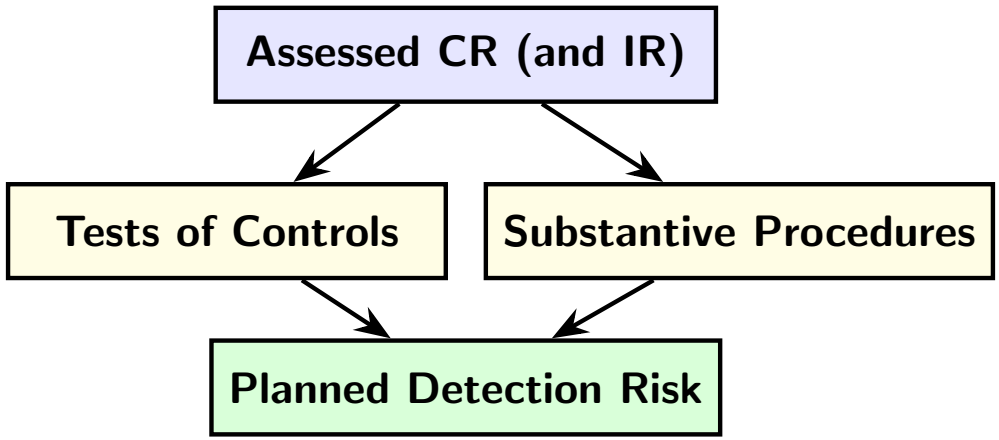
2. A _____ exists if one or more control deficiencies are less severe than a material weakness, but important enough to merit attention by those charged with governance.[28]
   - **A)** Potential misstatement
   - **B)** Significant weakness
   - **C)** Significant deficiency
   - **D)** Fraud symptom

[27] C
[28] C

Control Risk and Audit Planning

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

- **Higher CR** $\Rightarrow$ lower allowable **DR** $\Rightarrow$ more **substantive testing**
- **Lower CR** $\Rightarrow$ higher allowable **DR** $\Rightarrow$ less **substantive testing**



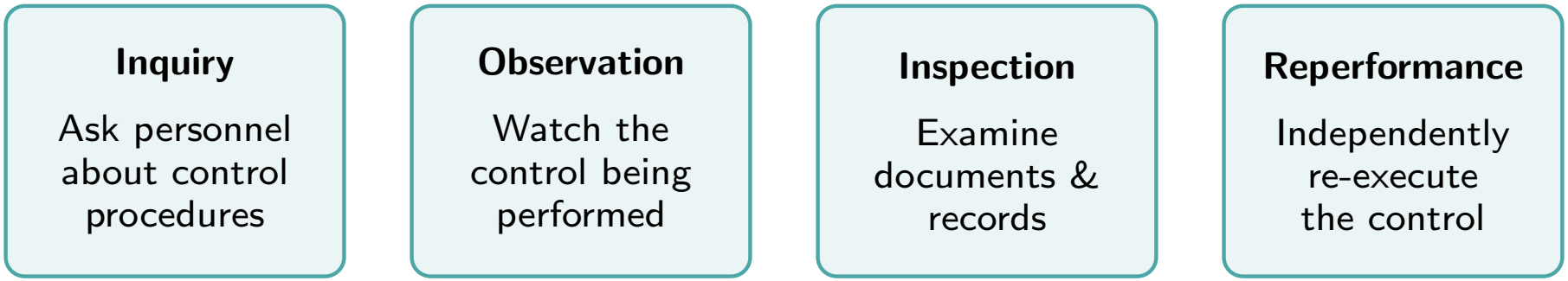
Step 3: Tests of Controls

Tests of Controls

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

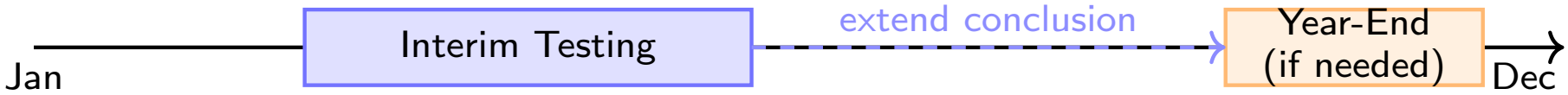
- Auditors perform tests of controls when they **plan to rely on controls** to reduce substantive testing.
- Indeed, auditors would like to reduce substantive testing by relying on controls while maintaining acceptable audit risk.

Methods: Tests of Controls



- **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:** **Interim testing** common
  $\rightarrow$ extend conclusion to year-end with limited additional work

- **Manual vs. Automated:**
  - **Automated** controls: consistent $\Rightarrow$ prior-year reliance possible[29]
  - **Manual** controls: variable $\Rightarrow$ more frequent testing required[30]

[29] assuming no changes to the control; still should be tested every three years under Auditing Standards.
[30] likely to include human error; so should be tested every year.

Tests of Controls vs. Substantive Procedures

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

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

If not effective, auditors will **increase** the extent of substantive procedures to compensate.

In the end, the ultimate goal is to maintain the desired level of **audit** risk.

Practice: Tests of Controls

1. Tests of controls are[31]
   - **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.[32]

3. [T/F] Auditing standards require auditors to test some prior-year controls each year to ensure rotation throughout a three-year period.[33]

[31] **A**
[32] **F**
[33] **T**

Table of Contents

Internal Control Communication

LO 5-5

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

Communicating IC Deficiencies[35]

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 **MW**.
- If a deficiency, or a combination of deficiencies in IC is less severe than a **MW**, it is a **SD**.
- Audit team must communicate both SD and MW to the MGT, BOD, and AC in writing.[34]

[34] MGT: Management; BOD: Board of Directors; AC: Audit Committee

[35] **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[36]

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.

[36] cannot obtain sufficient evidence

Table of Contents

Concluding Remarks

Internal controls should be:

- **designed** properly to prevent and detect MM and
- **operated** effectively as intended.

Effective internal controls would:

- **reduce** the need for substantive testing.

Reporting: Opinions on ICFR:

- Public firms with public float of \$75M+: required by **SOX 404(b)**
- 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 controlactivities 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