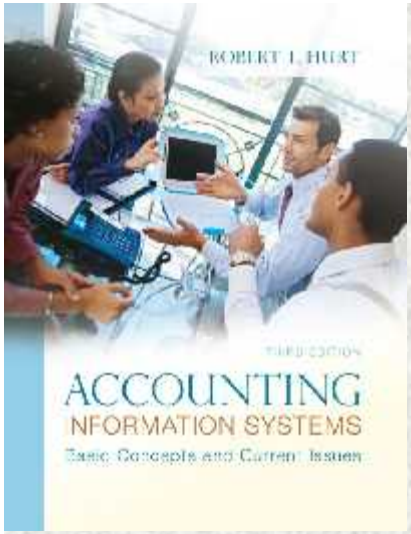


Chapter 3

Internal Controls

Outline

- Expected outcomes
- Definition and purposes
- Risk exposures
- COSO framework
- Examples
- Risk / control matrix

Expected outcomes

- Define internal control and explain its importance in the AIS.
- Explain the basic purposes of internal control and its relationship to risk.
- Describe and give examples of various kinds of risk exposures.
- Prepare a simple risk / control matrix.
- Summarize and explain the importance of COSO's Internal Control—Integrated Framework.
- Critique existing internal control systems and design effective internal controls.

Definition and purposes

- 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 the following categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.

Definition and purposes

- Important elements of the definition
  - **Process** nature of internal control
  - **Widespread responsibility** throughout the organization
  - Use of the term “entity” to describe a **broad range of organizations**
  - **Reasonable** assurance, which considers the cost / benefit constraint

Definition and purposes

- Internal control has four main purposes.
- Many people focus on the first two only, but all four are important.
- Note the **verbs** used with each purpose.

- Safeguard assets.
- Ensure reliable financial reporting.
- Promote operating efficiency.
- Encourage compliance with management directives.

Risk exposures

- Many organizations determine their internal controls by thinking about their risk exposures.
- Brown's taxonomy is one good way to think about risk.
- Four broad categories
  - Financial risk
  - Operational risk
  - Strategic risk
  - Hazard risk
- A given risk can "fit" into multiple categories.

Risk exposures

- Financial risk
  - Market risk
  - Credit risk
  - Liquidity risk
- Operational risk
  - Systems risk
  - Human error risk
- Strategic risk
  - Legal and regulatory risk
  - Business strategy risk
- Hazard risk
  - Directors' and officers' liability risk

Risk exposures

- **Lecture break 3-1**

  Do an Internet search for other risk taxonomies. Work with a group of three to five students to summarize one or them. Compare and contrast it to the Brown taxonomy. Which do you think is better? Why?

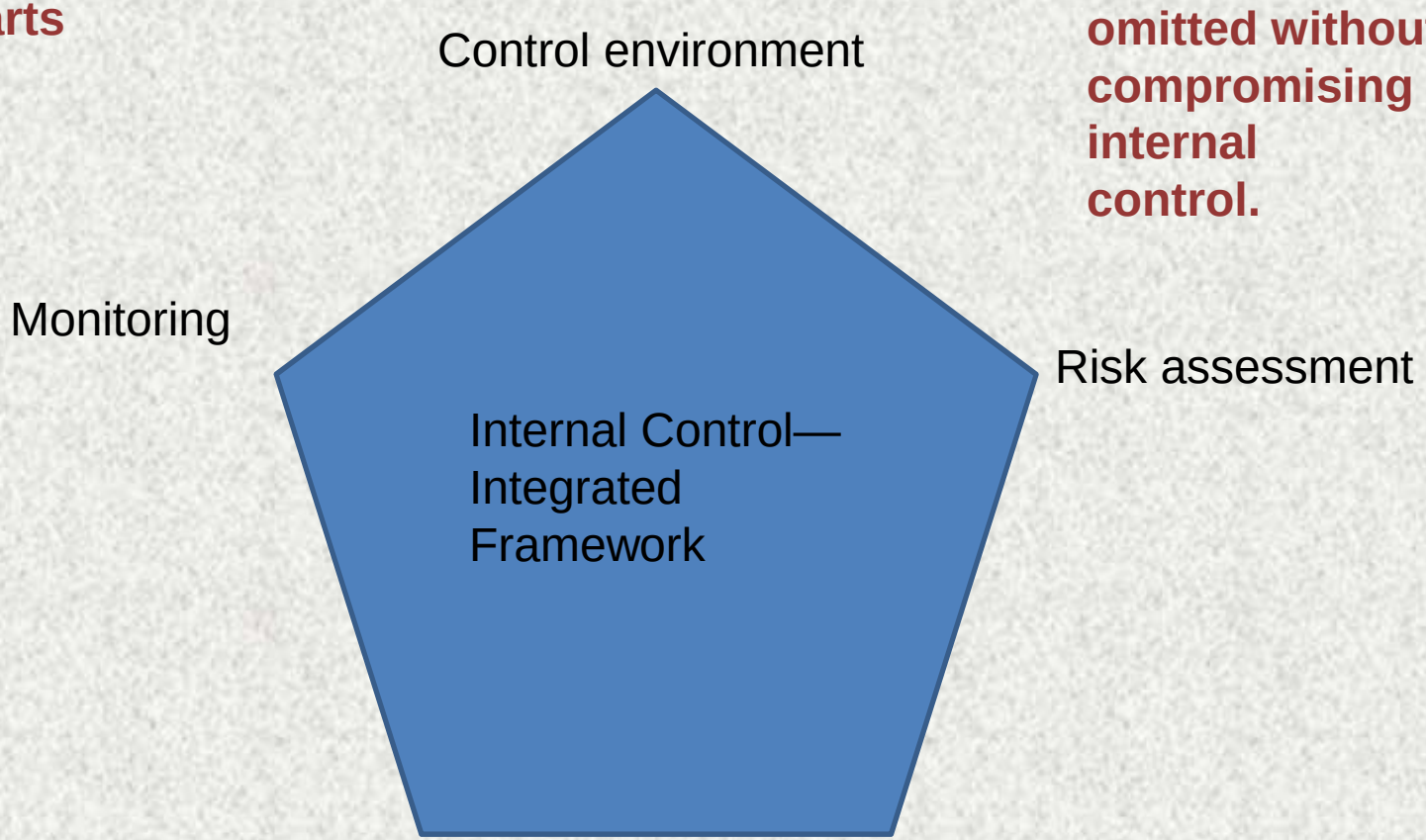
COSO framework

- **C**ommittee **o**f **S**ponsoring **O**rganizations of the Treadway Commission on Fraudulent Financial Reporting: www.coso.org
- Published many documents, the first of which was Internal Control—Integrated Framework.
- Late in 2010, COSO announced plans to update the framework.

COSO framework

The five parts form an integrated whole.

None can be omitted without compromising internal control.



Examples

- Discussed in the text
  - Separation of duties
  - Document matching
  - Restrictive endorsement and daily deposit of checks
  - Bank reconciliation
  - User training
- Other examples
  - Password policies
  - Forced vacations
  - Job rotation
  - Biometric access to IT assets
  - Video surveillance

Risk / control matrix

- One good way to correlate risk exposures with internal controls
- Many formats, but some common information in all
- See Table 3.2 in the chapter or the relevant post on Dr. Hurt's AIS blog

Risk / control matrix

- **Lecture break 3-2**
  - Form a group of three to five students.
  - Suggest three examples of risk exposures for one of the following types of organizations:
    - Retail general merchandise store (e.g., Target)
    - Bank (e.g., Bank of America)
    - Restaurant / food service (e.g., Pizza Hut)
  - Prepare a risk / control matrix following the format of Table 3.2.

Classroom assessment

- In this lecture, we've examined the following topics:
  - Definition & purposes of internal control
  - Risk exposures
  - COSO framework
  - Examples
  - Risk / control matrix

- Write a one-minute paper on the most important idea you gleaned from today's session.