ACFE
Association of Certified Fraud Examiners
Together, Reducing Fraud Worldwide

Fraud Prevention and Deterrence

Corporate Governance

Corporate Governance

- Oversight responsibilities of different parties for an organization's direction, operations, and performance
- OECD definition:
  - Procedures and processes according to which an organization is directed and controlled
  - Distribution of rights and responsibilities
  - Lays down rules for decision-making

Corporate Governance

- *The Cadbury Report* stated that the purpose is "to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources"
- Solid CG practices are necessary when owners are not responsible for setting strategy or carrying out business activities
  - E.g., publicly traded companies

Corporate Governance Parties

- Board of directors and its sub-committees
  - Made up of individuals generally elected by the entity’s voting members
  - Includes:
    - Major shareholders or executives of the organization (*inside directors*) and/or
    - Individuals completely independent of the organization aside from their role on the board (*independent directors* or *outside directors*)
  - Middlemen between shareholders and management
- Management
  - Directing employees to carry out business activities
- Shareholders
  - Hold the BOD accountable

Role of Corporate Governance in Fighting Fraud

- Effective governance processes are the foundation of fraud risk management
- Lack of effective corporate governance undermines any fraud risk management program
- Active board participation is critical

Principals of Corporate Governance

- Accountability
  - From management to board to shareholders
- Transparency
  - Clarity, accuracy, completeness, and timeliness of financial statements
- Fairness
  - All stakeholders treated equitably and given just and appropriate consideration
- Responsibility
  - Fiduciary duties

OECD *Principles of Corporate Governance*

- Regarded as one of the hallmark sources of guidance for corporate governance practices for organizations throughout the world
- Nonbinding
- Must be adapted to different legal, economic, cultural circumstances
- Useful in developed and emerging markets

OECD *Principles of Corporate Governance*

- Promote transparent and fair markets and the efficient allocation of resources.
- Be consistent with the rule of law.
- Support effective supervision and enforcement.
- Protect shareholders' rights.
- **Ensure the equitable treatment of all shareholders.**
- Provide all shareholders with the opportunity to obtain effective redress.
- Create sound incentives throughout the investment chain.
- Enable stock markets to function in a way that contributes to good corporate governance.
- Recognize the rights of stakeholders established by law or through mutual agreements.
- **Encourage active cooperation** between corporations and stakeholders.
- **Ensure timely and accurate disclosure**.
- Ensure strategic guidance, effective monitoring, and accountability.

Establishing a Corporate Governance Framework

- There is no single model of good corporate governance—OECD
- Structure and practices vary widely according to specific needs of each organization
- Must be adaptable for changing legal, regulatory, institutional, and ethical environments
- Must be fluid

U.S.-Specific Corporate Governance Codes and Guidance

- CG requirements are found in legislative and regulatory requirements imposed upon corporations.
- Each state has laws governing those corporations registered in it.
- Public companies are subject to federal legislation (SOX), as well as regulation by securities industry oversight bodies (NYSE, NASDAQ).

Sarbanes-Oxley Act

- SOX Audit Committee
  - Sole responsibility for hiring, overseeing, and paying external auditors and for resolving any disputes that arise between the auditors and management
  - Also required to establish procedures (e.g., a hotline) for receiving, retaining, and dealing with complaints
  - Required to pre-approve all services to be performed by the external auditors

NYSE and NASDAQ Requirements

- Board composed by a majority of independent directors.
- Board must have a nominating/corporate governance committee, composed entirely of independent directors.
- Board must have a compensation committee.
- Board must have an audit committee.
- Company must have an internal audit function.
- Company must adopt and disclose a code of conduct and ethics for its directors, officers, and employees.

The Treadway Commission

- Formed to define the auditor's responsibility in preventing and detecting fraud
- Recommendations for Audit Committee:
  - Mandatory Independent Audit Committee
    - Made up of outside directors
  - Written Charter
    - Setting forth duties and responsibilities of Audit Comm.
  - Adequate Resources and Authority
    - For Audit Committee to carry out responsibilities
  - Audit Committee Members Should Be Informed, Vigilant, and Effective

Sample Prep Question

1. Which of the following is TRUE regarding a corporation's board of directors?

   A. The directors are elected by the company shareholders
   B. Individual directors can also be major shareholders or executives of the organization
   C. The directors represent the middlemen between the shareholders and management
   D. All of the above

Correct Answer: D

- A corporation's board of directors is made up of individuals generally elected by the shareholders. Elected directors might be major shareholders or executives of the organization (often referred to as *inside directors*), or they might be completely independent of the organization aside from their role on the board (often referred to as *independent directors* or *outside directors*). The directors represent the middlemen between the corporation's shareholders and those actually carrying out its activities (i.e., management), and act as guardians of the organization's resources and assets. As such, the board oversees business operations by assessing the strategy and underlying purpose of management's decisions and actions.

Sample Prep Question

2. Which of the following is NOT one of the core principles of sound corporate governance?

   A. Responsibility
   B. Transparency
   C. Independence
   D. Fairness

Correct Answer: C

- Most systems of corporate governance are focused on several core principles or values, which include:
  - Accountability
  - Transparency
  - Fairness
  - Responsibility

Sample Prep Question

3. Both the NYSE and NASDAQ have rules requiring listed companies to adopt and disclose a code of conduct for all employees and to report any waivers of the code for directors or officers.

   A. True

   B. False

Correct Answer: A

- Companies with securities listed on the NYSE are bound by the corporate governance requirements contained in the NYSE *Listed Company Manual*; similarly, the corporate governance standards issued as part of the NASDAQ Equity Rules apply to all entities with securities listed on the NASDAQ exchange. Both the NYSE and the NASDAQ rules include a requirement that listed companies adopt and disclose a code of conduct for all directors, officers, and employees. The rules for both exchanges also state that any waivers of the code of conduct for directors or officers must be approved by the board of directors and disclosed.

Fraud Prevention and Deterrence

Management's Fraud-Related Responsibilities

Responsibility for Fraud Prevention

- Vicarious or Imputed Liability
  - Corporations can be held liable for criminal acts of their employees if those acts are done in the course and scope of their employment and for the ostensible purpose of benefiting the organization.
  - A company cannot avoid liability by claiming ignorance.
  - The corporation can be held criminally responsible *even if those in management had no knowledge or participation.*

The COSO Report

- It is management's job to ensure that proper internal controls are in place to prevent fraud, as well as to detect it.
- Internal Control is a process . . . designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

  a) Effectiveness and efficiency of <u>operations</u>

  b) Reliability of financial and nonfinancial <u>reporting</u>

  c) <u>Compliance</u> with applicable laws and regulations

Committee of Sponsoring Organizations

- Identified five interrelated components of internal control:
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring

COSO

- The Control Environment
  - Sets the tone of an organization
  - Influences the control consciousness of the organization
  - Provides a foundation for all other control components
- Risk Assessment
  - An entity's identification and assessment of risks relevant to achieving control objectives
    - Clear **objectives**
    - Identifies risks to achievement
    - **Considers potential for fraud**
    - **Assesses changes**

COSO

- Control Activities
  - An entity's control policies and procedures
- Information and Communication
  - The exchange of information in a way that allows employees to carry out their responsibilities
- Monitoring
  - The process that assesses the control environment over time

Sarbanes-Oxley Act (SOX)

- Signed on July 30, 2002
- Increased responsibilities of management and auditors and accounting firms

Summary of SOX and SEC Releases

- Criminal and Civil Certifications of CEO and CFO
- *Civil Certification*
  - Personally reviewed report
  - No material misstatements
  - Financial info fairly presented
  - Responsible for designing, maintaining, and evaluating internal controls and have done so
  - Disclosed material weaknesses or any fraud involving management
  - Disclosed significant changes

Defining Internal Control

Internal control over financial reporting (ICFR) is defined as:

> *"A process designed … to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles…"*

Mgmt's Report on Internal Control (IC) Section 404

- Statement of management's responsibility for establishing and maintaining adequate IC
- Identifying framework that management used in assessment of the effectiveness of IC

Mgmt's Report on Internal Control (IC) Section 404

- Management's assessment of the effectiveness of IC as of the end of most recent fiscal year, including:
  - Disclosure of any material weaknesses identified in IC
  - Explicit statement if IC is effective
- Statement that independent auditor issued an attestation report covering management's assessment of IC

Code of Ethics

- Under SOX, public companies must disclose whether they have adopted a code of ethics for senior financial officers, and if not, explain their reasoning
- Details left to the company
- Rules do not specify any detailed requirements, particular language, compliance procedures, or sanctions
- Senior financial officers: principal executive officer, accounting officer, controller, etc.

Whistleblower Protections

- Civil liability
  - For retaliation against employee who provides information or assists in investigation of fraudulent activity
  - For retaliation for filing, testifying, participating, or otherwise assisting in a proceeding relating to violation of securities laws and regulations
  - Only covers employees of publicly traded companies

Whistleblower Protections

- Criminal liability
  - For retaliation against another party for providing information regarding an alleged federal offense to a law enforcement officer
  - Applies to anyone regardless of whether the company is publicly traded
  - Report must be made to law enforcement

Sample Prep Question

1. Which of the following parties is ultimately responsible for the prevention and detection of fraud within an organization?

   A. Board of directors
   B. Internal auditors
   C. Management
   D. External auditors

Correct Answer: C

- While many parties—including the board of directors, internal audit, and external auditors—play an important role in combatting fraud, management is ultimately responsible for the prevention and detection of fraud within an organization.

Sample Prep Question

2. According to the Committee of Sponsoring Organizations (COSO), the control environment of an organization:

   A. Is established by directors and senior management
   B. Sets the moral and ethical tone of the organization
   C. Provides the foundation for the overall internal control system
   D. All of the above

Correct Answer: D

- The *control environment* provides the foundation for the internal control system throughout the entire organization. Established by the directors and senior management, it sets the moral and ethical tone of an organization, which reinforces the importance of internal controls and expected standards of conduct.

Sample Prep Question

3. Under Section 404 of the Sarbanes-Oxley Act, public U.S. companies must include all of the following in their annual report EXCEPT:

   A. A statement identifying the framework used in performing the assessment of the effectiveness of internal controls over financial reporting
   B. A statement of management's responsibility for establishing and maintaining adequate internal controls over financial reporting
   C. A report explaining any discovered deficiencies in the company's internal controls over financial reporting
   D. Management's assessment of the effectiveness of the company's internal controls over financial reporting

Correct Answer: C

- Under Section 404 of the Sarbanes-Oxley Act, public U.S. companies must issue an internal control report within their annual report containing:
  - A statement of management's responsibility for establishing and maintaining adequate ICOFR
  - A statement identifying the framework used by management in performing the assessment of the effectiveness of ICOFR
  - Management's assessment of the effectiveness of the company's ICOFR
  - A statement that the independent auditor has issued an attestation report on management's assessment of the company's ICOFR

Association of Certified Fraud Examiners
Together, Reducing Fraud Worldwide

Fraud Prevention and Deterrence

Auditors' Fraud-Related Responsibilities

Private Securities Litigation Reform Act

- Audits must include:
  - Procedures designed to provide <u>reasonable</u> <u>assurance</u> of detecting illegal acts that would have a <u>direct</u> and <u>material</u> effect on the determination of financial statement amounts
  - Procedures designed to identify related-party transactions material to the financial statements or that require disclosure
  - Evaluation of ability to continue as going concern
- Illegal Act:
  - Any act or omission that violates any law, rule, or regulation having force of law

Private Securities Litigation Reform Act

- If an auditor "detects or otherwise becomes aware that an illegal act (whether or not perceived to have a material effect on the financial statements of the issuer) has or might have occurred," the auditor must:
  - Determine and <u>consider the possible effect</u> of the illegal act on the financial statements of the company, including any contingent monetary effects such as fines, penalties, and damages
  - <u>Inform the appropriate level of management</u> "as soon as practicable"
  - Ensure that the audit committee is <u>adequately informed</u> of the illegal acts that have been detected unless such acts are "clearly inconsequential"

AU 240 and AU 200, Responsibilities and Functions of Independent Auditor

"The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements as a whole are free of material misstatement, whether due to fraud or error."

AU 240 Ten Main Sections

1. Description and characteristics of fraud
2. Importance of exercising professional skepticism
3. Discussion among engagement personnel regarding risk of material misstatement due to fraud
4. Obtaining information needed to identify risks of material misstatements due to fraud

AU 240 Ten Main Sections

5. Identifying risks that may result in material misstatements due to fraud
6. Assessing the identified risks after taking into account an evaluation of the entity's programs and controls
7. Responding to the results of the assessment

AU 240 Ten Main Sections

8. Evaluating audit evidence
9. Communicating about fraud to management, the audit committee, and others
10. Documenting the auditor’s consideration of fraud

Descriptions and Characteristics of Fraud

- Auditors must be interested in all acts that result in material misstatements
- Two relevant types of misstatements are those:
  - Arising from fraudulent financial reporting
  - Arising from misappropriation of assets

Discussion Among Engagement Personnel

- Audit team should discuss the potential for material misstatements due to fraud.
- Discussion should include “brainstorming” among the audit team members about the following:
  - How and where they believe the entity’s financial statements might be susceptible to fraud
  - How management could perpetrate or conceal fraud
  - How assets of the entity could be misappropriated

Discussion Among Engagement Personnel

- Should also include consideration of known external and internal factors affecting the entity that might:
  - Create incentives/pressures for management and others to commit fraud.
  - Provide the opportunity for fraud to be perpetrated.
  - Indicate a culture or environment that enables management and others to rationalize committing fraud.

Obtaining Information

- Make inquiries of management and others to obtain their views on risks of fraud.
- Consider any unusual or unexpected relationships that have been identified.
- Consider whether one or more fraud risk factors exist.
- Consider other information that may be helpful in the identification of risks of material misstatement due to fraud.

Risk Assessment Procedures

- Identify Risks of Misstatement
  - Type
  - Significance
  - Likelihood
  - Pervasiveness
- Overall Responses to Risks of Misstatement
  - Assignment of personnel and supervision
  - Accounting principles
  - <u>Predictability</u> of auditing procedures

PCAOB Auditing Standard No. 5

- SOX 404 mandates that management assess and report on effectiveness of Internal Controls
- Although objectives are not identical, IC audits and Financial Statement audits should be <u>integrated</u>
- Using a Top-Down Approach
  - Begins at the financial statement level to understand risks
  - Then focuses on entity-level controls and works down

PCAOB Auditing Standard No. 5

- Fraud Considerations
  - Controls over significant unusual transactions
  - Controls over journal entries and adjustments made during the end of the period reporting process
  - Controls over related-party transactions
  - Controls related to significant management estimates
  - Controls that mitigate the motivations for, and pressures on, management to engage in fraud
- At close of integrated audit, auditor may choose to issue single or separate report

Internal Auditor Responsibilities

- Internal auditors play a key role in helping organizations prevent and detect fraudulent activity
- Close proximity and better understanding of company

IIA Standards and Practice Guides

- 1220—Due Professional Care
  - Care and skill—Prudent and competent
- 2120—Risk Management
  - Evaluate risk exposures:
    - Achievement of the organization's strategic objectives
    - Reliability and integrity of financial and operational information
    - Effectiveness and efficiency of operations
    - Safeguarding of assets
    - Compliance with laws, regulations, and contracts
  - IA must evaluate <u>potential for occurrence</u> of fraud and how the organization <u>manages risk</u>

IIA Standards and Practice Guides

- IPPF—Practice Guide: IA and Fraud
  - <u>Consider risks</u> in assessment of internal control design and determination of audit steps to perform
  - Sufficient knowledge of fraud to identify red flags
  - <u>Be alert</u> to opportunities that could allow fraud, such as control deficiencies
  - Evaluate whether management is <u>actively retaining responsibility</u> for oversight
  - <u>Evaluate the indicators</u> of fraud and decide whether any further action is necessary or whether an investigation should be recommended
- IA role in investigations varies by organization

GAO Auditing Standards

- Standards for audits of government organizations, programs, activities, and functions, and of government assistance received by contractors, nonprofit organizations, and other non-government organizations, have been developed by the Comptroller General of the United States, Government Accountability Office (GAO)
- Known as the “Yellow Book”

GAO Auditing Standards

- The Yellow Book promulgates standards for two types of audits:
  - Financial audits
  - Performance audits
- Also contains standards covering attestation engagements, such as examinations and reviews, and other non-audit services performed on government organizations and programs

GAO Auditing Standards

- Performance Standards
  - Fraud-related responsibilities of an auditor performing generally accepted government auditing standards (GAGAS) engagement are fundamentally the same as those required of auditors under AU Section 240.
  - However, they include expanded requirements related to considerations of noncompliance and abuse during a financial audit.

GAO Auditing Standards

- Standards for Performance Audits
- 6.32 When information comes to the auditors' attention indicating that fraud that is significant within the context of the audit objectives might have occurred, auditors should extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and, (2) if so, determine its effect on the audit findings. If the fraud that might have occurred is not significant within the context of the audit objectives, the auditors may conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

Sample Prep Question

1. The primary purpose of AU Section 240 is to:

   A. Establish standards for auditors in fulfilling their responsibilities related to fraud during a financial statement audit

   B. Establish auditors as being primarily responsible for the prevention and detection of fraud within an organization

   C. Emphasize that the primary responsibility for establishing internal controls rests with auditors

   D. All of the above

Correct Answer: A

- Auditors have the responsibility to plan and perform an audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. The auditing standard codified in AU Section 240, *Consideration of Fraud in a Financial Statement Audit*, establishes standards and provides guidance to auditors in fulfilling that responsibility, as it relates to fraud, in conducting a financial statement audit. While this standard focuses on the auditor's consideration of fraud in an audit of financial statements, management is primarily responsible for the prevention and detection of fraud.

Sample Prep Question

2. The Private Securities Litigation Reform Act of 1995 requires that each audit of the financial statements of a public company include procedures designed to provide _____________ assurance of detecting illegal acts that would have a direct and material effect on the determination of the financial statement amounts.

   A. Absolute
   B. Reasonable
   C. Material
   D. None of the above

Correct Answer: B

- The Private Securities Litigation Reform Act of 1995 drastically changed the procedures and proof required in securities fraud cases. Among other requirements, each audit of the financial statements of a public company must include procedures designed to provide *reasonable* assurance of detecting illegal acts that would have a direct and material effect on the determination of financial statement amounts.

Sample Prep Question

3. According to The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, internal auditors must apply the care and skill of an expert whose primary responsibility is investigating fraud.

   A. True

   B. False

Correct Answer: B

- Internal Auditing Standard 1220 states that internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. The standard also states, however, that due professional care does not imply infallibility.