Chapter 2, Managing Risk: The Role of Auditing and Assurance

Questions

1. What are the three broad objectives of a traditional audit conducted under generally accepted auditing standards?

2. What fourth broad objective applied to audits of SEC-registered public companies in the United States?

3. Describe three different auditing standards and their source.

4. To achieve effective risk management, what must be recognized about the *nature* of risks?

5. What are the eight components of enterprise risk management according to COSO's 2004 ERM framework? Define each component.

6. Although all eight components of enterprise risk management according to COSO's 2004 ERM framework are important, which is most critical and why?

7. Depending on the nature of the risk and the resources available, an organization can deal with risks in four ways. Identify and explain these four responses to risk.

8. What is a control activity? What factors influence the effectiveness of a control mechanism?

9. Distinguish between risk, information risk and business risk.

10. Why is external auditing important to risk management?

11. What are some indications of ineffective risk management that the auditor may see as signs of potential risks?

12. Compare the management perspective of risk management to the auditor's perspective of risk management.

13. Compare the management perspective of information reliability to the auditor's perspective of information reliability.

14. Compare the management perspective of performance measurement to the auditor's perspective of performance measurement.

15. What management activities are the focus of the auditor when evaluating internal control over financial reporting?

16. What determines the extent to which an auditor is expected to examine internal control over financial reporting?

17. Describe the three phases of an integrated audit.

18. Because management is responsible for providing reliable financial information to stakeholders, management, management must implement an effective process for maintaining control over financial reporting. What must management do in achieving this?

19. Auditors must assess whether management has identified and tested appropriate controls. What are these controls?

20. What is the auditor's primary concern when testing the effectiveness of internal control over financial reporting?

21. Define and describe enterprise risk management.

Problems

22. Compare and contrast management controls and business process controls using a national grocery store chain as an example.

23. *Explain compliance risks, using the example of a paint manufacturing company.*

24. Why are external auditors interested in risk management?

25. Explain the evolution from the traditional financial statement audit to the modern integrated audit.

26. Depending on the nature of the risk and the resources available, an organization can deal with risks in four ways. Identify and explain these four responses to risk using *a local as an example.*

27. In a business environment, risk can be addressed four ways: avoidance, acceptance, sharing, and reduction. For Taco Bell, identify how each of the following risks can be addressed by one of these four options.
    a. Customers might not want to buy deep fried products.
    b. Lawsuits might be brought upon the company should customers contract e-coli.
    c. Franchisees might not follow corporate guidelines for advertising and promotion.
    d. Food preparation could differ from location to location.

ANSWERS

Questions

1. What are the three broad objectives of a traditional audit conducted under generally accepted auditing standards?
   a. Evaluate whether the financial statements are presented in accordance with GAAP and free of material misstatements.
   b. Evaluate the possibility of fraudulent financial reporting.
   c. Evaluate the likelihood that the organization will continue as a going concern.

2. What fourth broad objective applied to audits of SEC-registered public companies in the United States?
   a. Evaluate internal control over financial reporting.

3. Describe three different auditing standards and their source.
   a. In general, audits in the United States are conducted under the guidance of *Generally Accepted Auditing Standards* promulgated by the American Institute of CPAs (AICPA).
   b. Audits of publicly-listed companies in the United States are conducted under *Auditing Standards* issued by the Public Company Accounting Oversight Board (PCAOB).
   c. *International Standards on Auditing* are established by the International Auditing and Assurance Standards Board (IAASB).

4. To achieve effective risk management, what must be recognized about the *nature* of risks?
   a. Risks affect organizations in various ways (e.g., achieving strategy, performing effectively, reporting faithfully, and complying with regulations fully).
   b. Risks are interrelated (e.g., one risk event may trigger other risk events).
   c. Risks can only be managed through intervention by management or other stakeholders.

5. What are the eight components of enterprise risk management according to COSO's 2004 ERM framework? Define each component.
   a. The *internal environment* refers to an organization's general philosophy and approach to risk management.
   b. *Objective setting* refers to the set of organizational objectives supported through risk management (these may include strategic, operations, reporting, and compliance).
   c. *Event identification* refers to the organization's ability to identify circumstances and events that represent potential risks that are relevant to the organization's objectives.
   d. *Risk assessment* refers to the identification, evaluation and prioritization of potential risks that emanate from the identified events.

e. *Risk response* refers to an organization's basic plan for avoiding, accepting, reducing, or sharing risks.
f. *Control activities* are the specific activities an organization undertakes to reduce risk.
g. *Information and communication* refers to an organization's need for information so that it can effectively respond to risk, and an organizations production and distribution of relevant and timely information, all of which help determine the effectiveness of risk management.
h. *Monitoring* refers to the continuous evaluation of risk management efforts that is necessary to assure effectiveness over time.

6. Although all eight components of enterprise risk management according to COSO's 2004 ERM framework are important, which is most critical and why?
   a. The *internal environment* is critical because it lays the foundation for all other elements of risk management. Specifically, the internal environment reflects the attitudes, approach, and competence of management with regard to enterprise risk management. If owners can hire competent and honest management whose personal goals are aligned with the owners, many other forms of control may be reduced.

7. Depending on the nature of the risk and the resources available, an organization can deal with risks in four ways. Identify and explain these four responses to risk.
   a. *Avoidance:* The organization may attempt to avoid some risks by carefully choosing not participate in certain markets, products or activities.
   b. *Acceptance:* The organization may choose to accept some risks as an inevitable, unavoidable result of business decisions.
   c. *Sharing:* An organization may transfer (at a cost) all or part of a set of risks to another party, such as through insurance, strategic alliances, and/or hedging transactions.
   d. *Reduction:* An organization may attempt to reduce many risks by designing and implementing proactive policies, procedures, and processes.

8. What is a control activity? What factors influence the effectiveness of a control mechanism?
   a. Control activities refer to any actions taken by a company or individual to reduce the likelihood or significance of risk. However, very few risks can be reduced to zero, no matter what approaches or combination of approaches are selected.
   b. Different control responses have different degrees of effectiveness and costs to implement. Two key attributes influence the effectiveness of a control mechanism: diagnosticity and objectivity. Diagnosticity refers to the ability of a control activity to provide a reliable and timely warning of potential problems. Objectivity refers to potential bias inherent in the execution of a control.

9. Distinguish between risk, information risk and business risk.
   a. A *risk* is a threat to an organization that reduces the likelihood that the organization will achieve one or more of its objectives.

b. *Information risk*, which is particularly relevant to auditors, is the risk that information used in decision making is inaccurate or insufficient.
c. *Business risk* refers specifically to potential risks arising from the company's external environment and internal activities that may have a negative impact on its operations and overall performance.

10. Why is external auditing important to risk management?
    a. The external auditors provide an objective check on the reliability and fairness of financial information. However, they also provide assurance over other aspects of an organization such as providing owners with corroborative evidence that control is operating effectively, and giving managers feedback on improving internal control over financial reporting for their own purposes. Auditors are uniquely qualified to provide such assurance because they possess the professional skills to provide highly diagnostic services, while maintaining objectivity.

11. What are some indications of ineffective risk management that the auditor may see as signs of potential risks? *{Note: Instructors may wish to specify a minimum number of responses.]*
    a. Lack of a formal enterprise risk management process
    b. Failure to monitor strategic risks
    c. Failure to adequately respond to identified risks
    d. Lack of reliable performance measurement data
    e. Inadequate information for monitoring processes
    f. Failure to respond to signs of problems and visible threats

12. Compare the management perspective of risk management to the auditor's perspective of risk management.
    a. Management must identify, assess, and prioritize risks that may negatively impact the organization. Management evaluates each risk with regard to its likelihood of occurring and the significance of its impact.
    b. The auditor discerns whether management has identified all possibly significant risks and accurately assessed their likelihood and significance. The auditor wants to be sure to management is not omitting or underestimating risks because those risks will not be effectively managed.

13. Compare the management perspective of information reliability to the auditor's perspective of information reliability.
    a. Management must ensure that information systems are designed to provide appropriate performance measurement data to assess the past, present, and future likelihood or significance of various risks.
    b. The auditor must assess the reliability of information processing and reporting. The auditor needs a vast amount of information, most of which comes from internal processes. The auditor wants the most reliable information so that fewer problems can be expected during the engagement.

14. Compare the management perspective of performance measurement to the auditor's perspective of performance measurement.
    a. Management needs periodic information to use for reviewing performance. Performance measures are needed to indicate how the organization is performing and to warn early of potential problems.
    b. The auditor uses performance measurement information to judge management's control of risks. Data measured over a period of time will indicate when conditions change or risks arise that may lead to problems during the engagement.

15. What management activities are the focus of the auditor when evaluating internal control over financial reporting?
    a. The auditor focuses on internal control over financial reporting which is the subset of enterprise risk management that pertains to the processes and procedures that management has established to
        i) Maintain records that accurately reflect the company's transactions
        ii) Prepare financial statements and footnote disclosures for external purposes and provide reasonable assurance that receipts and expenditures are appropriately authorized
        iii) Prevent or promptly detect unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

16. What determines the extent to which an auditor is expected to examine internal control over financial reporting?
    a. This depends on whether the audit is being performed under the rules of a traditional GAAS audit or the PCAOB rules for an Integrated Audit. The effort required to evaluate internal control is much more extensive in an Integrated Audit.

17. Describe the three phases of an integrated audit.
    a. *Examination of management's assessment of internal control over financial reporting.* An auditor's evaluation of management's assessment of internal control involves understanding the process undertaken by management to assess control effectiveness, including the results of tests of controls for all significant transactions, accounts, and disclosures. To this end, the auditor assesses whether management has identified and tested appropriate controls.
    b. *Examination of the actual effectiveness of internal control over financial reporting.* The auditor's responsibility is to evaluate and test the effectiveness of internal control over financial reporting as of the end of the fiscal year. The auditor's primary concern is whether ineffective controls could lead to material misstatements in the financial statements. The auditor's understanding of internal control over financial reporting should include the design of controls and whether they have been placed in operation.
    c. *Examination of the financial statements (similar to a GAAS audit).* The final phase of the audit process is similar for a traditional GAAS audit and an Integrated Audit, although the extent of the examination will vary because of the deep understanding of internal control over financial reporting an auditor

develops in an Integrated Audit. One difference is that the auditor may be able to perform more focused tests of transactions, accounts, and disclosures in an Integrated Audit, concentrating on areas of the financial statements where the risk of error is highest, and reducing tests in areas considered to have a low risk of error.

18. Because management is responsible for providing reliable financial information to stakeholders, management must implement an effective process for maintaining control over financial reporting. What must management do in achieving this?
    a. Management must formally accept the responsibility for the effectiveness of the company's internal control over financial reporting
    b. Management must evaluate the effectiveness of the company's internal control over financial reporting using suitable criteria
    c. Management must support its evaluation with sufficient evidence, including documentation
    d. Management must provide a written assessment about the effectiveness of the company's internal control over financial reporting as of the end of the fiscal year

19. Auditors must assess whether management has identified and tested appropriate controls. What are these controls?
    a. Controls over financial reporting processes, from initialization of transactions to financial statement presentation
    b. Controls over accounting policies, from selection to evaluation of how they were applied
    c. Fraud prevention and detection controls
    d. Controls over non-routine transactions and estimates that typically are associated with errors or fraud
    e. Company-level controls (management's attitude about misstatements, management's risk assessment process, centralized processing and controls, and monitoring controls such as the audit committee, internal audit, etc.).
    f. Controls over period-end financial reporting process.

20. What is the auditor's primary concern when testing the effectiveness of internal control over financial reporting?
    a. The auditor's primary concern is whether ineffective controls could lead to material misstatements in the financial statements. The auditor's understanding of internal control over financial reporting should include the design of controls and whether they have been placed in operation.

21. Define and describe enterprise risk management.
    a. According to COSO, enterprise risk management is a process, enacted by an entity's board of directors, management, and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, to manage risks to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives.
    b. ERM is a formal process that affects all levels of an organization.

c. ERM is an iterative, continuous process that involves identifying, assessing, and managing key risks that threaten an organization's strategic, operational, compliance, and reporting objectives at all levels of an organization.

Problems

22. Compare and contrast management controls and business process controls using a national grocery store chain as an example.
    a. *Management controls* reflect the efforts to reduce strategic risk that are the responsibility of senior management. The management of the national grocery store chain will establish corporate objectives and strategies, and then evaluate the financial performance of the organization and progress towards those objectives. They can use these controls to motivate employees to strive for goals and behave within established boundaries of conduct and activities, or provide feedback about potential problems or risks that the organization may need to address. Example management controls the management of a grocery store chain might set include assessing strategic risks, monitoring business processes, reacting to changing circumstances (such as extreme weather or shifts in the economy), establishing codes of conduct (such as non-discrimination in hiring), setting budgets, and evaluating performance of personnel or business units or product groups.
    b. *Business process controls* are designed to assure that the activities within a process are performed efficiently and effectively, addressing operational risk. Business process controls define how tasks are performed within an organization and comprise the policies and procedures that determine how internal processes operate on a day-to-day basis. The business process controls may dictate who has the authority to execute a transactions (such as which employees can process a refund), how documents are to be processed (such as how coupons must be handled), how information is to be collected and reported (such as how the inventory system and point of sale system work together), and how problems are to be handled (such as what a cashier should do when an item will not scan at checkout).

23. *Explain compliance risks, using the example of a paint manufacturing company.*
    a. Compliance risks affect to an organization's need to fulfill government regulations or oversight. These risks are managed by identifying internal decision makers who are responsible for significant regulatory mandates, and then providing them with relevant and reliable information so that they can monitor conditions related to those mandates. Most organizations have a process in place to focus on the core regulatory requirements they face. For example, a paint manufacturer will need to maintain compliance with the regulations of the Occupational Health and Safety Agency to ensure safety of workers and those of the Environmental Protection Agency, particularly relative to emissions and wastewater.

24. Why are external auditors interested in risk management?

a. First, the auditor provides assurance about information generated from the organization's processes. Financial statements contain feedback about the strategic decisions and results of an organization. Consequently, to evaluate the information the auditor must understand the organization's strategic position, threats and plans, and information systems reliability. The auditor must evaluate whether reported financial statement results reflect economic reality in accordance with generally accepted accounting principles. Therefore, the auditor must understand the economic reality surrounding the information in the financial statements, including management's approach to risk management.
b. Second, an auditor may participate in the risk management process. For example, some companies outsource monitoring activities related to internal control and internal auditing. Replacement of internal sources of monitoring with external auditing may increase the objectivity of the control process without reducing the ability of the control to diagnose problems. Outside auditors may be better trained or can afford to be specialists; therefore outsourced monitoring may be more effective than in-sourced monitoring. Of course, to maintain objectivity, the auditor of the external financial statements should not perform internal auditing activities.
c. Third, the auditor may be engaged to provide assurance that one or more components of the risk management process are operating efficiently and effectively. At the same time, the auditor may provide guidance when the risk management process is weak or flawed.

25. Explain the evolution from the traditional financial statement audit to the modern integrated audit.
    a. Traditionally, a financial statement audit focuses almost entirely on whether the numbers and disclosures in a financial report are fairly presented. However, as modern commerce has become increasingly global and complex, and businesses larger and more sophisticated, the traditional approach to auditing has evolved, a development necessitated by the auditing scandals of recent years.
    b. These events have increased both operational risk and information risk so that the auditor is expected to expand their audit beyond the traditional view. Specifically, external auditors now have greater involvement with the client's internal controls over financial reporting. This is seen as improving the auditor's ability to detect potential risks and ensure the financial statements reflect them. It also reinforces the belief that companies have a responsibility to stakeholders to design strong systems of internal control. In addition, it requires auditors to have an expanded skill set concerning risk management and control effectiveness.
    c. Audits involve an examination of the information included in the financial statements. Additionally, audits also include evaluation of the quality of the internal accounting system that generates financial information.

26. Depending on the nature of the risk and the resources available, an organization can deal with risks in four ways. Identify and explain these four responses to risk using a local company as an example. *{NOTE: Instructors may wish to specify a single*

company. Answers will vary due to the company chosen, but all must address each of the following issues.}

a. *Avoidance:* The organization may attempt to avoid some risks by carefully choosing not participate in certain markets, products or activities.
b. *Acceptance:* The organization may choose to accept some risks as an inevitable, unavoidable result of business decisions.
c. *Sharing:* An organization may transfer (at a cost) all or part of a set of risks to another party, such as through insurance, strategic alliances, and/or hedging transactions.
d. *Reduction:* An organization may attempt to reduce many risks by designing and implementing proactive policies, procedures, and processes.

27. In a business environment, risk can be addressed four ways: avoidance, acceptance, sharing, and reduction. For Taco Bell, identify how each of the following risks can be addressed by one of these four options (avoid, accept, insure or reduce).
    a. Customers might not want to buy deep fried products.
    b. Lawsuits might be brought upon the company should customers contract e-coli.
    c. Franchisees might not follow corporate guidelines for advertising and promotion.
    d. Food preparation could differ from location to location.

    Answer:

    a) Avoid: Taco Bell does not sell deep fried products, such as French fries like most other fast food chains, possibly because they do not have a process for incorporating the necessary equipment to efficiently serve customers, and possibly because customers who desire Mexican food do not desire French fries.

    b) Insure: Taco Bell carries liability insurance policies regarding lawsuits stemming from spoiled food served to customers.

    c) Accept: Taco Bell issues franchises instead of owning restaurants. An inherent risk of franchising is placing control of operations in the hands of franchisees all over the world. Should franchises not follow established policies, the trademark can be negatively affected by associated negative publicity.

    d) Reduce: Taco Bell uses strict operating policies for its franchises to help ensure that the product tastes the same in every restaurant. Specific equipment must be purchased by franchisees and preparation procedures must occur according a formal plan.