Turner/Accounting Information Systems, 2e
Solutions Manual
Chapter 3

Concept Check

1. b
2. c
3. a
4. d
5. d
6. b
7. b
8. a
9. a
10. d
11. c
12. b
13. c
14. d

Discussion Questions

15. (SO 1) *Management is held accountable to various parties, both internal and external to the business organization. To whom does management have a stewardship obligation and to whom does it have reporting responsibilities?* Management has a stewardship obligation to the shareholders, investors, and creditors of the company, i.e., any parties who have provided funds or invested in the company. Management has a reporting responsibility to business organizations and governmental units with whom the company interacts.

16. (SO 2, 4) *If an employee made a mistake that resulted in a loss of company funds and misstated financial reports, would the employee be guilty of fraud? Discuss.* No, a mistake, or unintentional error, does not constitute fraud. In this situation, there is no theft or concealment, so fraud does not exist.

17. (SO 2, 3) *Do you think it is possible that a business manager may perpetrate fraud and still have the company's best interest in mind? Discuss.* Student responses may vary. Those agreeing that it is possible may refer to the fraud triangle and note that the incentive may be job-related (such as opportunities to produce enhanced

financial statements, which may increase the company's stock price, increase compensation, avoid firings, enhance promotions, and delay bankruptcy) and the rationalization may involve plans to make restitution. On the other hand, some students may reject the notion that management fraud could be in a company's best interest, as it puts the company at great risk. When frauds are discovered, they are often devastating due to the financial restatements and loss of trust.

18. (SO 7) *Distinguish between internal and external sources of computer fraud.* Employees are the source of internal computer fraud. When employees misuse the computer system to commit fraud (through manipulation of inputs, programs, or outputs), this is known as internal computer fraud. On the other hand, external sources of computer fraud are people outside the company or employees of the company who conduct computer network break-ins. When an unauthorized party gains access to the computer system to conduct hacking or spoofing, this is known as external computer fraud.

19. (SO 7) *Identify and explain the three types of internal source computer fraud.* The three types of internal source computer fraud are input manipulation, program manipulation, and output manipulation. Input manipulation involves altering data that is input into the computer. Program manipulation involves altering a computer program through the use of a salami technique, Trojan horse program, trap door alteration, etc. Output manipulation involves altering reports or other documents generated from the computer system.

20. (SO 7) *Describe three popular program manipulation techniques.* The salami technique accomplishes a fraud by altering small "slices" of computer information. These slices of fraud are difficult to detect because they are so small, but they may accumulate to a considerable amount if they are carried out consistently across many accounts. This is often accomplished by rounding or applying minor adjustments. The perpetrator typically steals the amounts represented by these slices or uses them to his or her benefit.

    A Trojan horse program is a small, unauthorized program within a larger, legitimate program, used to manipulate the computer system to conduct a fraud. For example, a customer account may be automatically written off upon the processing of a new batch of transactions.

    A trap door alteration involves misuse of a valid programming tool, a trap door, to commit fraud. Trap doors are unique hidden entrances to computer programs that are written into the software applications to provide a manner of testing the systems. Although they should be removed prior to implementation, they may remain to provide a tool for misusing the system to perpetrating fraud.

21. (SO 7) *Distinguish between Internet spoofing and e-mail spoofing.* Internet spoofing involves a person working through the Internet to access a computer network while pretending to be a trusted source. The packet of data containing the Internet

protocol (IP) address contains malicious data such as viruses or programs that capture passwords and log-in names. E-mail spoofing bombards employee e-mail accounts with junk mail intended to scam the recipients.

22. (SO 10) *What are the objectives of a system of internal control?* The objectives of an internal control system are as follows:

- To safeguard assets from fraud or errors
- To maintain accuracy and integrity of accounting data
- To promote operational efficiency
- To ensure compliance with management directives

23. (SO 10) *Name and distinguish among the three types of internal controls.* The three types of internal controls are preventative controls, detective controls, and corrective controls. Preventative controls are designed to avoid fraud and errors by stopping any undesired acts before they occur. Detective controls help employees uncover or discover problems that may exist. Corrective controls involve steps undertaken to correct existing problems.

24. (SO 10) *Identify the COSO report's five interrelated components of internal controls.* According to the COSO report, there are five interrelated components of internal control: the control environment, risk assessment, control activities, information and communication, and monitoring.

25. (SO 10) *Name the COSO report's five internal controls activities.* According to the COSO report, there are five internal control activities: authorization of transactions, segregation of duties, adequate records and documents, security of records and documents, and independent checks and reconciliations.

26. (SO 10) *Distinguish between general and specific authorization.* General authorization is a set of guidelines that allows transactions to be completed as long as they fall within established parameters. Specific authorization means that explicit approval is needed for that single transaction to be completed.

27. (SO 10) *Due to cost/benefit considerations, many business organizations are unable to achieve complete segregation of duties. What else could they do to minimize risks?* Close supervision may serve as a compensating control to lessen the risk of negative effects when other controls, especially segregation of duties, are lacking.

28. (SO 10) *Why is a policies and procedures manual considered an element of internal control?* Formally written and thorough documentation on prescribed policies and procedures should establish clarity and promote compliance within a business organization, thus providing an important element of internal control. The policies and procedures should cover both manual and automated processes and control measures, and must be communicated to all responsible parties within the company.

29. (SO 10) *Why does a company need to be concerned with controlling access to its records?* Securing and protecting company records is important to ensure that they are not misused or stolen. Unauthorized access or use of records and documents allows the easy manipulation of those records and documents, which can result in fraud or a concealment of fraud.

30. (SO 10) *Many companies have mandatory vacation and periodic job rotation policies. Discuss how these practices can be useful in strengthening internal controls.* Mandatory vacations and periodic job rotation policies provide for independent monitoring of the internal control systems. Internal control responsibilities can be rotated so that someone is monitoring the procedures that are typically performed by someone else, which enhances the effectiveness of those procedures.

31. (SO 10) *Name the objectives of an effective accounting system.* An effective accounting system must accomplish the following four objectives:

    - Identify all relevant financial transactions of the organization.
    - Capture the important data of these transactions.
    - Record and process the data through appropriate classification, summarization, and aggregation.
    - Report the summarized and aggregated information to managers.

32. (SO 10) *What does it mean when information flows "down, across, and up the organization"?* A business organization must implement procedures to assure that its information and reports are communicated to the appropriate management level. This communication is described by COSO as "flowing down, across, and up that organization". Such a communication flow assists management in properly assessing operations and making changes to operations as necessary.

33. (SO 10) *Provide examples of continuous monitoring and periodic monitoring.* Any ongoing review activity may be an example of continuous monitoring, such as a supervisor's examination of financial reports and a computer system's review modules. An example of periodic monitoring is an annual audit performed by a CPA firm or a cyclical review performed by internal auditors.

34. (SO 10) *What are the factors that limit the effectiveness of internal controls?* It is not possible for an internal control system to provide absolute assurance because of the following factors that limit the effectiveness of internal controls:

    - Flawed judgments
    - Human error
    - Circumventing or ignoring established controls

    In addition, excessive costs may prevent the implementation of some controls.

35. (SO 11) *Identify and describe the five categories of the AICPA Trust Services Principles.* The AICPA Trust Services Principles are divided into the following five categories of risks and controls:

    - Security. Security is concerned with the risk of unauthorized physical and logical access, such as breaking into the company's facilities or computer network.
    - Availability. Availability is concerned with the risk of system interruptions or failures due to hardware of software problems such as a virus.
    - Processing integrity. Processing integrity is concerned with the risk of inaccurate, incomplete, or improperly authorized information due to error or fraud.
    - Online privacy. Online privacy is concerned with the risk of inappropriate access or use of a customer's personal information.
    - Confidentiality. Confidentiality is concerned with the risk of inappropriate access or use of company information.

36. (SO 11) *Distinguish between the Trust Services Principles of privacy and confidentiality.* Both privacy and confidentiality are concerned with the risk of in appropriate access or use of information. However, privacy is focused on protecting the privacy of a customer's personal information; whereas confidentiality is focused private information about the company itself and its business partners.

37. (SO 10) *Identify the four domains of high-level internal control.* As set forth in Appendix B, COBIT establishes four domains of high level control objectives. These include planning and organization, acquisition and implementation, delivery and support, and monitoring.

Brief Exercises

38. (SO 2, 3) *What possible motivation might a business manager have for perpetrating fraud?* Management might be motivated to perpetrate fraud in order to improve the financial statements, which may have the result of increasing the company's stock price and increasing incentive-based compensation. Altered financial information might also have the effect of delaying cash flow problems and/or bankruptcy, as well as improving the potential for business transactions such as mergers, borrowing, stock offerings, etc.

39. (SO 5) *Discuss whether any of the following can be examples of customer fraud:*

    - *An employee billed a customer twice for the same transaction.* This is not an example of customer fraud; rather, the customer is being defrauded in this scenario. This is an example of employee fraud (assuming that the double-billing was intentional and the resulting cash receipts are stolen by employees).

- *A customer remitted payment in the wrong amount.* This may be an example of customer fraud, assuming that the payment was made as a deceptive tactic to avoid the full amount of the customer's liability.
- *A customer received merchandise in error, but failed to return it or notify the sender.* Although this scenario involves a customer's improper receipt of goods, it would not be considered customer fraud since it was the result of an error. Regardless of whether the error was committed by the company or the customer, deception is a required element of fraud.

40. (SO 7) *Explain the relationship between computer hacking and industrial espionage. Give a few additional examples of how hacking could cause damage in a business.* Computer hacking is the term commonly used for computer network break-ins. Hacking may be undertaken for various purposes, including theft of proprietary information, credit card theft, destruction or alteration of data, or merely thrill-seeking. Industrial espionage is the term used for theft of proprietary company information. Although computer hacking provides one method of conducting industrial espionage, a computer is not always required to steal company information. Fraudsters trying to conduct industrial espionage may also resort to digging through the trash in order to gain information about a target company.

41. (SO 9) *What are some ways in which a business could promote its code of ethics?* The best way for a company to promote its code of ethics is for its top managers to live by it on a day-to-day basis. If the code is well documented and adhered to by management, others in the organization are likely to recognize its importance. Furthermore, if discipline and/or discharges are applied to those who violate the code, this will serve as a strong message regarding the importance of the code.

42. (SO 10) *Describe why the control environment is regarded as the foundation of a business's system of internal control.* The control environment is regarded as the foundation of a system of internal controls because it sets the tone of an organization and influences the control consciousness of its employees. Thus, the tone at the top flows through the whole business organization and affects behavior at every level. It also provides the discipline and structure of all other components of internal control. COSO identifies the tone set by management as the most important factor related to providing accurate and complete financial reports.

43. (SO 10) *Think of a job you have held, and consider whether the control environment was risky or conservative. Describe which you chose and why.* Student responses will vary. Characteristics of a risky control environment include absence of a code or ethics or lack of enforcement of a code of ethics, aggressive management philosophy and operating style, overlapping duties and vague lines of authority, lack of employee training, and an inactive board of directors. On the other hand, a conservative control environment is characterized by a rigidly enforced code of ethics, a conservative management philosophy and operating style, clearly established job descriptions and lines of authority, a focus on employee training and organizational development, and an accountable and attentive board of directors.

44. (SO 10) *Identify the steps involved in risk assessment. Do you think it would be effective for an organization to hire external consultants to develop its risk assessment plan?* The steps involved in risk assessment include:

- Identify the sources of risk, both internal and external.
- Determine the impact of such risks in terms of finances and reputation.
- Estimate the likelihood of such risks occurring.
- Develop an action plan to reduce the impact and probability of identified risks.
- Execute the action plan on an ongoing basis.

It would not likely be effective for an organization to hire consultants to develop its risk assessment plan because company-specific experience and expertise are needed in order to do this work effectively. For instance, members of management who are actively involved in day-to-day operations and reporting will likely have the best ability to identify risks, determine the impact of those risks, and estimate the likelihood of occurrence of such risks. Although a consultant may be useful in assisting with the development and implementation of the action plan, the first three steps of the risk assessment process would likely depend upon the working knowledge of members of the company's management.

45. (SO 10, 11) *Discuss the accuracy of the following statements regarding internal control:*

- *The more computerized applications within a company's accounting system, the lower the risk will be that fraud or errors will occur.* It is not necessarily true that extensive computerized application will lower a company's risk of fraud. This is because computerized systems also increase vulnerabilities such as unauthorized access, business interruptions, and inaccuracies. The technological complexities that accompany sophisticated computer applications call attention to the need for extensive internal controls to reduce the risk of fraud and errors.
- *The more involved top management is in the day-to-day operations of the business, the lower the risk will be that fraud or errors will occur.* It is certainly true that the tone at the top (the tone set by top management) is the most important factor of internal control. Accordingly, it can be implied that involved managers would promote strong internal controls. However, although this is *often* true, it will be true *only* when top management acts with integrity, exemplifying and enforcing its code of ethics, maintaining a conservative approach to operations and financial reporting, and cultivating clear communications and responsibilities.

Problems

46. (SO 10) *Identify whether each of the following accounting positions or duties involves authorization, recording, or custody:*

- *cashier* - Custody
- *payroll processor* - Recording
- *credit manager* - Authorization
- *mailroom clerk* - Custody
- *data entry clerk* - Recording
- *deliver paychecks* - Custody
- *deliver the bank deposit* - Custody
- *prepare the bank reconciliation* - Recording
- *check signer* - Authorization
- *inventory warehouse supervisor* - Custody
- *staff accountant* - Recording

47. (SO 10) *Identify whether each of the following activities represents preventative controls, detective controls, or corrective controls:*

- *job rotation* - Detective
- *preparation of a bank reconciliation* - Corrective
- *segregation of duties* - Preventative
- *recalculating totals on computer reports* - Detective
- *use of passwords* - Preventative
- *preparing batch totals for check processing* - Detective
- *establishing a code of ethics* - Preventative
- *use of a security guard* - Preventative
- *verifying source documents before recording transactions* - Preventative
- *matching supporting documents before paying an invoice* - Preventative
- *independent review of accounting reports* - Detective
- *performing comparisons of financial statement items* - Detective

48. (SO 10) *Shown is a list of selected sources of internal control guidelines, given in order of issuance, followed by a list of primary purposes. Match each guideline with its primary purpose.*

I. *Foreign Corrupt Practices Act* – b. Prevented bribery and established internal control guidelines.
II. *COSO* – d. Established internal control concepts based on comprehensive study.
III. *SAS 99* – a. Required auditors to focus on risks and controls and to conduct audits with skepticism.
IV. *Sarbanes-Oxley Act* – c. Curbed fraud by requiring additional internal control reporting within annual reports.
V. *Trust Services Principles* – e. Established essential criteria for evaluating reliability of business systems.

a. Required auditors to focus on risks and controls and to conduct audits with skepticism.
b. Prevented bribery and established internal control guidelines.

c. *Curbed fraud by requiring additional internal control reporting within annual reports.*
d. *Established internal control concepts based on comprehensive study.*
e. *Established essential criteria for evaluating reliability of business systems.*

49. (SO 1, 3, 10) *Using a search engine on the Internet, find articles or descriptions of the collapse of Enron. The collapse began in November 2001, and many articles appeared over the next two to three years. Required:*

a. *Briefly describe the fraud that occurred.* Student responses are likely to vary, but should focus on the accounting frauds which attempted to hide the company's debt and losses. For instance, Enron created special purpose entities (related partnerships) for the purpose of off-balance sheet financing. Other deceptive transactions are known to have taken place for the sole purpose of creating false financial results, such as transactions involving the sale and buy-back of barges near year-end and prepaid commodities deals that were never delivered.
b. *Discuss what you see as weaknesses in the control environment.* It is likely that students will focus on the tone at the top, and conclude that management did not set a good example of the company's code of ethics. They may also provide evidence of aggressive management practices.

50. (SO 3) *Using a search engine on the Internet, search for articles on fraud that occurred in 2000 to 2002 in the following companies:*
Adelphia
Enron
Global Crossing
WorldCom
Xerox

Try to locate articles or information about stock prices, how the fraud was conducted. You might wish to look at the following websites: edgar.sec.gov, www.hoovers.com and www.forbes.com

Required:

a. *Find information to help you complete the following table:* Students are not likely to find all of this information, but what they do find may help them better understand the massive size and scope of these frauds. Some of the stock prices or loss to investors can be found by web searches. For example, the Xerox stock prices can be found by searching on Xerox, fraud and "stock price".

Company Name	Brief Description of Fraud	Position of Those Conducting Fraud	Stock Price when fraud was uncovered	Stock Price one year later	Shares outstanding	Loss to Investors
Adelphia	Off balance sheet financing,	CEO, CFO, VP of Operations				~$750 mil.

	inflated earnings, improper use of company funds	(Rigas family members)				
Enron	Off balance sheet financing through special purpose entities, inflated earnings	CEO (Ken Lay), CFO (Andrew Fastow), Pres./CEO (Jeff Skilling)	$90	$0.70		
Global Crossing	Inflated revenue through network capacity swaps, mis-management and excessive spending	Founder (Gary Winnick), CEO, CFO, and Pres. Of Finance				
WorldCom	Off-balance sheet credit, inflated earnings through improper capitalization of operating expenses	CFO & Controller (possibly CEO)	$60	$0.20		
Xerox	Accelerated revenue recognition on leased assets	Senior executives	$11.24	$4.30		

b. *Discuss the common characteristics that you see in each of these examples.* Most of these frauds involved misstated financial statements involving inflated earnings and off-balance sheet financing. Most of these frauds were perpetrated by members of top management, including top ranking financial executives.

51. (SO 3) *Using a search engine on the Internet, search for information on the following two companies, which were paying bribes in foreign countries:* Student responses are likely to vary, but the information below highlights the main facts of these cases.

Siemens:

a. How it was discovered. The Siemens frauds were discovered after being exposed by a middleman/consultant who helped carry out some of the transactions to pay bribes and kickbacks to government officials in exchange for being awarded contracts in foreign countries. These types of bribery transactions were being carried out for years and in countries all over the globe. It was only a matter of time before investigators began examining the suspicious transactions.

b. *The end result of the investigation.* In 2008, Siemens pleaded guilty to criminal violations of the corrupt practices act, and has paid over $1.6 billion in fines and settlements. In late 2011, civil bribery charges were brought against several former Siemens executives.
c. *What you think the company might have done to prevent this, or lessen the impact.* These frauds involved high-ranking company officials, so internal controls should have been enhanced through practicing tone at the top. All of the funds and bank accounts that were established to carry out these acts should have been under the supervision of top executives. Senior managers at Siemens assumed that they would be supported by top executives, but they found out that they were wrong. After the bribes were discovered, Siemens worked hard to quickly remove many senior managers and reform company policies; however, there should have been controls in place to prevent these actions much sooner; it should have provided more thorough corporate governance and management oversight.
d. *What you learned about the Foreign Corrupt Practices Act.* The FCPA is enforced by the SEC and seeks to root out companies who engage in corrupt practices.

Johnson & Johnson:

a. *How it was discovered.* The J&J frauds were discovered internally and were reported to the SEC. Most of the frauds involved paying bribes to European doctors and hospital administrators in exchange for using J&J medical devices. It also paid kickbacks to Iraq to obtain contracts under the United Nations Oil for Food Program.
b. *The end result of the investigation.* J&J paid over $70 million in civil and criminal fines. Its penalties were reduced because of the level of cooperation the company provided throughout the investigation.
c. *What you think the company might have done to prevent this, or lessen the impact.* Like Siemens, top management should have had better controls in place from the beginning, rather than having to work so hard on damage control and subsequent compliance efforts. In particular, if the cash payments had been more closely monitored, these bribes and kickbacks could have been detected and stopped at a much earlier point in time.
d. *What you learned about the Foreign Corrupt Practices Act.* The FCPA is enforced by the SEC and seeks to root out companies who engage in corrupt practices.

Cases

52. *Fraud at Wooten's city hall. Required:*

a. *Which internal control activity was violated in order for Mr. Peterman to perpetrate this fraud?* A case could be made for any or all of the internal control activities were violated in this scenario. With regard to authorization, it can be said that Mr. Peterman abused his authority by circumventing the established controls in order to carry out these transactions on his own. His interference in the mailroom procedures made it impossible for any segregation of duties to occur. There was apparently inadequate security and documentation for the assets and transactions with which he was involved, and there was no one willing to come forward to review or reconcile these transactions.
b. *Do you consider this case to be an example of management fraud or employee fraud?* Although it involves misappropriation of assets, which is typically an employee fraud, this was conducted by the chief financial officer. Accordingly, it would be considered a management fraud. It is not likely that Mr. Peterman would have been able to carry out his fraud if it had not been for his high-ranking position, which apparently prevented anyone from stopping him.
c. *Was the city's procedural manual adequate for prescribing internal controls to prevent this type of fraud? Why or why not?* Although the case states that written guidelines were in place regarding the mailroom and bank deposit policies, requirements for logging checks received and performing an independent verification of receipts, these guidelines were obviously not followed when Mr. Peterman stepped in. Rather than being a problem with the documented policies, this case seems to present a situation marked by circumvention of controls.
d. *Why do you think no one reported the unusual mailroom practices of Mr. Peterman? To whom would such a violation be reported?* Since Mr. Peterman was the highest ranking financial officer in the organization, employees who suspected misconduct likely believed that there was no one with authority over Mr. Peterman to whom the problem could be reported. If management is involved in fraud, it should be brought to the attention of the board of directors. In the case of a municipality, the problem could be reported to the chief administrator, mayor, or the city's advisory council.
e. *Do you think a business in Wooten could be guilty of customer fraud if it agreed to deliver its payments to Mr. Peterman personally rather than send them to the city's mailing address?* A business that agreed to deliver its payments to Mr. Peterman personally would not likely be guilty of fraud. Customer fraud requires the intent to deceive, so unless the business had knowledge or was otherwise involved in Mr. Peterman's fraud scheme, it would not be guilty of customer fraud.
f. *The comments made by the neighbor CFO express which type of limitation of internal control systems discussed in this chapter?* The limitation of small staff size typically means that the business organization does not have sufficient resources to accomplish segregation of duties. Accordingly, controls can be easily circumvented. The comment

regarding the tight operating budget reflects upon the cost/benefit limitations of internal controls.

53. *Coupon accounting abuse. Required:*

a. *Discuss whether the situation described can happen to a company with a good control environment.* This situation would not be likely to happen to a company with a good control environment. In a conservative control environment, management would not place so much emphasis on profitability, would not likely tie compensation to profitability and then give employees responsibility for preparing their own profitability reports, and would have likely provided for other controls (such as supervision and review of Larry's figures).
b. *Describe any steps a company could take to prevent such abuse.* If the firm was going to compensate brand managers based on profitability of their brands, then those managers should not have responsibility for preparing their own profitability reports. Rather, an independent accounting function should be in place to account for Larry's brands. In addition, independent reconciliations should be performed with specific emphasis on risky financial items such as coupon drops.
c. *List those parties who might be harmed by this situation.* The following parties are likely to be harmed as a result of Larry's fraud:
    - investors and creditors who rely upon the fair presentation of the firm's financial statements as a basis for business decisions
    - shareholders to whom the firms owes a stewardship obligation, especially as they are deceived with respect to the firm's current financial status
    - fellow employees in the firm who will begin the next year with an inflated expense for the coupon drop (and whose compensation will be tied to financial performance)
    - fellow employees who share in Larry's bonus pool, whose bonuses would have been larger had Larry's figures been accurate
d. *Do you consider this example to be management fraud or employee fraud? Describe how it fits the definition of your choice.* This case describes management fraud, as it involves misstatement of financial records, which is typically perpetrated by managers who are attempting to realize benefits (such as increased compensation).

54. *Ethical dilemma involving a CEO. Required:*

a. *Discuss whether Mr. Brocamp's violation of corporate ethics policy affects or reflects the control environment of the company.* Yes, Mr. Brocamp's actions affect the control environment of Mega Motor Company. As its CEO, Mr. Brocamp has primary responsibility for setting the tone at the top and living by the code of ethics. If others in the organization are aware

of this violation, it sends the message that the code of ethics is not important. This is likely to lead to other problems, including fraud.

b. *Since the violation is personal in nature, should Mr. Brocamp have been forced to resign?* Since the code of ethics specifically prohibits personal relationships between managers and members of their management chain, then Mr. Brocamp should be held accountable for his actions. Even though it could be argued that the relationship did not affect his ability to perform his job effectively, the company must have thought otherwise when it established its code of ethics.
c. *Should Bozeman State have hired him to teach business strategy courses?* Student responses are likely to vary and may provide the basis for an interesting class discussion. Some students may agree that someone who violated a company ethics policy should not be teaching students about the proper management of organizations. Others may agree that faculty members are not questioned about their personal lives and that Mr. Brocamp's wealth of experience is beneficial to students.

55. *Ethical dilemma involving mail order fraud. Required:*

a. *Discuss which type of fraud is involved in this case, from the perspective of the mail order company.* This case presents an example of customer fraud, as Janie deceived the mail order company. She obtained property and lied about it in order to avoid the corresponding liability.
b. *Which of the AICPA Trust Services Principles most closely related to this situation?* Processing integrity is the Trust Services Principle that most closely relates to this situation. Since Janie provided false information and the company had no way to substantiate it, inaccurate information was processed and became part of the financial records of the company.
c. *Describe a preventative control that could be performed by the carrier to avoid the possible recurrence of this type of fraud.* If the carrier had documented the address where the package was dropped off or obtained a signature from Janie's neighbor at the time of delivery, the deception would have been prevented. This would have provided documentation of the delivery, which could have been investigated.

56. *Ethical dilemma involving charitable fundraiser. Required:*

a. *Do you think Evan's actions were justified? What would you have advised him to do in this situation?* No, Evan's actions were not justified because he did not use the donated funds for their intended purpose. Since Evan represented to the donors that the monies were to be used for a charitable purpose, he had an ethical obligation to fulfill that commitment. Even though he invested more time than he planned, he knew that his efforts were not to be compensated. This is a variation of an employee fraud. As a representative of a charitable cause, he carried out a cash receipts theft for his personal gain.

b. *What internal control activities could the fraternity have implemented in order to prevent Evan's actions?* The fraternity should have required its treasurer to handle the cash receipts related to this fundraising campaign. This would separate the custody of the cash receipts from the recordkeeping that Evan was conducting.
c. *Can you think of a detective control that could uncover the omission of the $200 check?* A review of all receipts – or in this case, acknowledgement letters – could be performed and reconciled to the cash contributions records. Unless Evan concealed the letter written to the donor of the $200 that he stole, such a reconciliation procedure would uncover the difference.