Review Questions

1. The 2008 *Report to the Nation* estimated that U.S. organizations lose seven percent of their annual revenues to fraud, which equates to approximately US $994 billion based on the 2008 U.S. gross domestic product.
2. The *Fraud Guide* defines fraud as "any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain."
3. The American Institute of Certified Public Accountants (AICPA) states that fraudulent financial reporting can be accomplished by:
   - Manipulating, falsifying, or altering accounting records or supporting documents from which the financial statements are prepared.
   - Misrepresenting, or intentionally omitting from, the financial statements events, transactions, or other significant information.
   - Intentionally misapplying accounting principles relating to amounts, classification, manner of presentation, or disclosure.
4. The Association of Certified Fraud Examiners (ACFE) states that an act of occupational fraud:
   - Is clandestine (that is, secretive and suspicious).
   - Violates the perpetrator's fiduciary duties to the victim organization.
   - Is committed for the purpose of direct or indirect financial benefit to the perpetrator.
   - Costs the employing organization assets, revenues, or reserves.
5. The fraud triangle highlights the three elements of fraud: perceived need/pressure, perceived opportunity, and rationalization. Fraud perpetrators want to relieve real or perceived pressure to show performance (for example, generating the attitude that when you can't "make" the numbers, you just "make up" the numbers), they need to see ample opportunity so that they can carry out the fraud with ease (for example, nobody's watching the store, the employee is trusted completely), and most importantly, they need to rationalize their action as acceptable (for example, I'm doing it for the good of the company).
6. According to the *Fraud Guide*, the board's oversight should generally include:
   - A general understanding of fraud-related policies, procedures, incentive plans, etc.
   - A comprehensive understanding of the key fraud risks.
   - Oversight of the fraud risk management program, including the controls that have been implemented to manage fraud risks.
   - Receiving and monitoring reports that provide information about fraud incidents, investigation status, and disciplinary actions.
   - The ability to retain outside counsel and experts when needed.
   - Directing the internal audit function and the independent outside auditor to provide assurance regarding fraud risk concerns.
7. A successful integrated fraud program will typically have the following components:
   - *Commitment* by the board and senior management. This commitment should be formally documented and communicated throughout the organization.
   - *Fraud awareness* activities that help employees understand the purpose, requirements, and responsibilities of the program. These activities may include any or all of the following: written communications to all employees, oral communications during organization-wide meetings, postings on the organization's internal website and external web page, and formal training programs.
   - *An affirmation process* that requires employees to affirm periodically, typically annually, that they understand and are complying with policies and procedures.
   - *A conflict disclosure* protocol or process that helps employees self-disclose potential or actual conflicts of interest. This would also include a means for timely resolution of matters that have been disclosed.
   - *Fraud risk assessment*, which helps to identify all reasonable fraud scenarios. This is discussed further in the next section.
   - *Reporting procedures and whistleblower protection* that provide a well-known and easy avenue for individuals, whether inside or outside the organization, to report suspected violations or incidents.
   - *An investigation process* that ensures all matters undergo a timely and thorough investigation, as appropriate.
   - *Disciplinary and or corrective actions* that address noncompliance with established policies and help deter fraudulent behavior.
   - *Process evaluation and improvement* to provide quality assurance that the program will continue to meet its objectives.
   - *Continuous monitoring* to ensure the program consistently operates as designed.
8. The three key steps are :
   1) Identify inherent fraud risks.
   2) Assess impact and likelihood of the identified risks.
   3) Develop responses to those risks that have a sufficiently high impact and likelihood to result in a potential outcome beyond management's tolerance.
9. In a perfect world, an organization would prefer to prevent frauds from occurring. Once a fraud has occurred there are costs to investigate the incident, remediate the conditions that allowed the fraud to occur, and take the appropriate disciplinary actions. These costs may be financial, reputational, or other. However, the real world is not perfect and it is neither possible nor cost effective to prevent all fraud incidents.
10. According to the *Report to the Nation*, anonymous tips are the most common method of fraud detection.
11. The final stage focuses on investigating, reporting, and correcting the suspected fraud incidents.
12. Golden believes that financial reporting fraud perpetrators are either "greater good oriented" or "scheming, self-centered" types.
13. An internal audit function can:
    - Conduct fraud awareness training.
    - Assess the design of antifraud programs and controls.
    - Test the operating effectiveness of antifraud controls.
    - Investigate improprieties and whistleblower complaints.
    - Conduct full-fledged investigations.

CHAPTER 8
FRAUD RISKS & CONTROLS
Illustrative Solutions

Multiple-choice Questions

1. **B** is the best answer. Predication, sometimes called "credication," refers to the existence of reason to believe that the allegation of fraud has a strong enough basis to require the formal launching of an investigation. Fraud examiners would not typically consent to commencing an investigation without predication (per the ACFE).
2. **A** is the best answer. The *Report to the Nation* identified that corruption occurred in 27 percent of reported fraud cases.
3. **D** is the best answer. While fraud perpetrators may feel they are smarter than most others, this is not a rationalization for committing fraud. Each of the others is considered a rationalization for fraud.
4. **D** is the best answer. The *Fraud Guide* cites the first three as responsibilities of all employees. Investigating suspicious activities should be conducted by those who are properly trained to do so.
5. **B** is the best answer. In this situation, a sales representative may deliver more units than the customer wants, and tell them they can return the units up to 90 days later. This may allow the sales representative to inflate their bonus. The other three answers also may be concerns for the company, but they are business risks and not necessarily fraud risks.
6. **C** is the best answer. Before conducting an investigation, it is best to understand all of the available facts against relevant criteria to determine whether an investigation, or some other form of follow-up, is warranted. Even if an investigation is warranted, a staff internal auditor probably does not have the experience to provide the support necessary to take action. Doing nothing is not acceptable as the accusations may be true, and lack of responsiveness sends a negative message to the organization about the tone at the top. The human resources department may need to be involved at some point, but they do not have the experience to assess whether this accusation justifies an investigation.
7. **A** is the best answer. Regardless of the amount, any asset of the organization that is directed for a use other than what was intended is a misappropriation of assets. The other answers may represent fraud, but they do not represent a misappropriation of assets.
8. **D** is the best answer. The first three are elements that can play an important role in preventing fraud, while the last would be considered a detective control.
9. **C** is the best answer. While all of these organizations are vulnerable to fraud, banks deal in cash, which is valuable to almost all individuals and subject to potentially the largest losses from fraud. Instructors may want to take the opportunity to discuss other outcomes of fraud, such as inadequate protection of customers' privacy. While C is still the best answer, it will provide students with greater insights into how one must consider the assets involved, the value of the assets, and the potential amounts that can be misappropriated.
10. **B** is the best answer. Such a control would serve to *prevent* an unauthorized change to critical payroll data, such as the pay rate. Some students may question why C is not an acceptable answer. This control may help *detect* unauthorized changes, but it will not prevent such changes. A and D are valid payroll controls, but they would not prevent unauthorized changes.
11. **C** is the best answer. This description of the internal auditor's responsibilities is consistent with The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*). For instance, IIA Standard 1210.A2 states, "Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud."
12. **B** is the best answer. The internal audit function is viewed as in-house "internal control experts" and should be consulted by senior management and the audit committee about the design and implementation of effective anti-fraud programs and controls. Management owns the fraud risk management process and is the most important line of defense against fraud. The legal function would be the best lead for an investigation of fraud involving potential violation of laws and regulations. Determining punishment is a role of management, not the internal audit function.

CHAPTER 8
FRAUD RISKS & CONTROLS
Illustrative Solutions

Discussion Questions

1. If the internal audit function is to be successful in delivering on its mandate (that is, as defined in the internal audit charter), it needs the endorsement of the audit committee and the full support of the management team. Addressing fraud risk can be particularly sensitive when one or more senior management executives may be involved in the perpetration of fraud. Under such circumstances, if the internal audit function lacks independence and autonomy, it would not be difficult for management suspected of fraud to demand that the internal audit function cease from undertaking any investigative activities. (This is exactly what happened at WorldCom, when the internal auditors were obstructed in their fraud investigation by the chief financial officer (CFO), who was perpetrating financial statement fraud). In other words, the "problem of serving two masters" (that is, the audit committee as well as the CEO, CFO, general counsel, controller, etc.) becomes most acute and challenging when the internal audit function engages in an "audit of management." In organizations for which the audit committee has become the central clearinghouse for key governance and financial reporting activities, it makes sense for the internal audit function to report directly to the audit committee. Indeed, this sort of reporting arrangement is quickly becoming a best practice and is highly recommended by The Institute of Internal Auditors (IIA).
2. The referenced OCEG Internal Audit Guide (IAG) can be accessed at www.oceg.org. The control environment provides the foundation for an effective system of internal controls. "Soft controls" such as "tone at the top," control consciousness, and a culture of integrity and ethics, are important aspects of the control environment. The absence of any such controls compromises the effectiveness of the entire system of internal controls.

   Having a whistleblower hotline, and deterring activities that are "illegal, unethical, or immoral," are certainly good practices, but they are by no means sufficient by themselves to prevent such activities, just as having a code of conduct is not enough. Application of the code of conduct must be monitored, employees must be asked to indicate in writing that they have read it, and any suspected violations of the code or instances of noncompliance must be tracked. In other words, the code of conduct must be part of a larger "ethics and compliance program" and must be seen as enforceable — only then will employees take it seriously. Most importantly, it must be recognized that even the most comprehensive practices in this regard can provide only reasonable, not absolute, assurance that material fraud will be prevented. Unfortunately, the motivated fraudster who adopts collusive tactics with others within and/or outside the organization will usually prevail.
3. Short definitions for each of the terms are furnished below (most of the asterisked* definitions are borrowed or heavily adapted from the *Encyclopedia of Fraud* by Joseph T. Wells, published in 2005 by the ACFE, Austin, Texas). Instructors may want to select a portion of the terms from this list to reduce the amount of research time students spend.

1) Bribery & kickbacks*: Bribery generally refers to public officials accepting cash, goods and services, or favors in exchange for influence. Kickbacks are undisclosed payments by outsiders to an organization's employees. Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and vendors.
2) Conflict of interest: Represents a broad class of scenarios that feature individual(s) possessing informational, relationship-based, position-based, and other undisclosed economic or personal advantages that could be used to illegitimately exploit others for personal gain or benefit. For example, internal auditors should not use "inside information" to trade in employer company stocks or bonds, lawyers must not represent both the plaintiff and the defendant, and independent outside auditors should not audit a company in which they are also stockholders.
3) Cooking the books: A colloquial expression that refers to intentionally altering the books of account to deceive others or engaging in financial statement fraud.
4) Self-dealing and corruption*: Occurs when a person is found to be on both sides of the same transaction (an obvious but perhaps undisclosed and unknown conflict of interest, see definition 2 above), and is able to fraudulently exploit those under the impression that the transaction is legitimate. Like bribery (definition 1 above), corruption in the public sector includes any act in which a public official or employee performs favors in exchange for money, goods and services, influence, or other reward.
5) Defalcation/embezzlement: Stealing money or assets from one's employer for personal use. Thus a cashier who "borrows" money from the till for gambling or horse racing is embezzling.
6) Fictitious revenues or expenses: Making up false journal entries for nonexistent economic transactions or events to inflate revenues or overstate expenses (for example, to reduce the organization's tax liability).
7) Identity theft: Involves the stealing of another's identity, including personally identifiable information (PII), and illegal and unauthorized use of it to appropriate money, assets, or property (for example, credit card fraud).
8) Industrial espionage: Espionage conducted for commercial purposes instead of national security purposes. It includes activities such as theft of trade secrets (see definition 21 below), bribery, blackmail, technological surveillance, and spying on commercial organizations. Governments can also be targets of industrial espionage — for example, to determine the terms of a tender for a government contract so that another tenderer can underbid.
9) Intentionally violating GAAP: Generally Accepted Accounting Principles (GAAP), which include those promulgated by the Financial Accounting Standards Board (FASB) in the U.S. and the International Financial Reporting Standards (IFRS) established by the U.K.-based International Accounting Standards Board (IASB), constrain the practice of accounting, particularly in complex areas. When organizations intentionally misinterpret or violate GAAP, this behavior is tantamount to financial statement misrepresentation or even fraud. In such circumstances, they are likely to have to restate the materially misstated financial statements based on the recommendation of the independent outside auditors and/or regulators such as the U.S. Securities and Exchange Commission (SEC).
10) Kiting: Building up balances in bank accounts by floating checks drawn against similar accounts in other banks.

CHAPTER 8
FRAUD RISKS & CONTROLS
Illustrative Solutions

11) Lapping*: The fraudster's version of "robbing Peter to pay Paul." Lapping is the recording of payment on a customer's account sometime after the receipt of the payment, so that cash stolen from one customer is covered with the receipt of cash from another customer.
12) Larceny: The theft of cash after the cash has already been recorded on the books, such as directly from a cash register or petty cash. (Note: Skimming refers to the theft of cash that has yet to be recorded in an organization's books of account.)
13) Breach of fiduciary duty: A "fiduciary" is expected to be extremely loyal to the person to whom they owe the duty (that is, the "principal"). They must not put their personal interests before the duty, and must not profit from their position as a fiduciary, unless the principal consents. The fiduciary relationship is highlighted by good faith, loyalty, and trust. The word itself originally comes from the Latin fides, meaning faith. In a negligence lawsuit, there are four elements to consider: duty, breach of duty, causation, and damages. For breach of duty, it must be decided whether or not the defendant, the one being accused of negligence, behaved in a way that a reasonable person would have under similar circumstances. If no duty is owed, then there is no negligence and no negligence damages are owed.
14) Misrepresentation of material facts: Misleading the reader or user of financial statements by distorting information presented by means such as suggestion falsi (suggestion of falsehood) or suppression veri (suppression of truth).
15) Money laundering: A process by which the origin of funds from illegal enterprises — drug smuggling, terrorist financing, corruption, fraud, and other acts — is concealed. Perpetrators, that is, those who change "black money into white money" (laundering), move the funds through various channels before reclaiming the funds from what appears to be a legitimate source.
16) Conspiracy: An act of working in secret to obtain some goal, usually with negative connotations. A criminal conspiracy might involve two or more people who "conspire" to break the law in the future to attain some gain.
17) Sham entities: Fictitious entities, such as shell companies or banks, that exist without any physical presence in any legal jurisdiction. Their fabrication is solely for the purpose of committing fraud.
18) Round-tripping: A form of barter, or a transaction in kind, that involves an organization selling an unused asset while at the same time agreeing to buy the same or similar assets at the same price. A common transaction among telecommunication and energy companies in the past decade to inflate the apparent size of a market, the SEC ruled such transactions as improper.
19) Forgery*: Committed by imitating a document or object (for example, another's signature) with the intent to deceive. Besides monetary gains, forgers might be motivated by status or personal reasons such as revenge.
20) False or manipulated travel and entertainment reimbursement claims*: The padding of expenses relating to travel and entertainment (T&E) reimbursement claims by employees traveling on organizational business. Such padding may involve mischaracterizing expenses, overstating expenses, creating fictitious expenses, multiple reimbursements, and including unauthorized and illegitimate expenses.
21) Theft of trade secrets: A form of industrial espionage whereby confidential information considered strategically or operationally important is obtained inappropriately by a competitor or

some other party. The loss of such information could adversely impact the organization, potentially threatening its ability to survive.

22) Topside journal entries: Journal entries recorded on the topside (for example, in consolidation) but which are not posted to the general ledger. Examples include journal entries used to increase accounts receivables and revenues or decrease accounts payable and expenses. Typically, this creates a discrepancy between the adjusted figures on the financial statements and the actual books and records and is equivalent to "cooking the books" (see definition 3 above).

23) Bid rigging*: A scheme in which a vendor is given an unfair advantage in an open competition for a certain contract. Bid-rigging schemes during the contract pre-solicitation, solicitation, and negotiation phases involve collusion between the buyer and one contractor/vendor, to the detriment of competing contractors in the bidding process (sometimes involving defective pricing).

24) Price fixing: When a group of companies that are otherwise rivals decide to operate as a cartel and "agree upon prices" to charge the customer for the same product or service. Usually such a concerted but covert attempt to fix, peg, discount, or stabilize prices is good for the sellers and bad for the customers (as it usually results in price gouging). Under U.S. laws, such collusion to keep prices artificially high is illegal.

25) Undisclosed side agreements: Agreements between two parties that benefit one or both parties, but are not disclosed to other parties who may have an interest in the transaction. For instance, when auto dealers accept a large delivery of cars at the end of a quarter or at year-end accompanied by an undisclosed side agreement with the automobile company that a significant proportion of unsold cars are to be returned shortly after the quarter- or year-end. This amounts to a knowing act and thus fraud.

26) Ghost employees: A classic method of inflating expenditures on construction contracts that involves the inclusion of "ghost employees" on payroll sheets. Needless to say, such employees are not officially on the work site, but may show up on payday to collect their checks. Also, this scheme may be used by supervisors to create a fictitious employee and then pocket the wages of the fictitious employee.

27) Backdating stock options, spring loading, and bullet dodging: Manipulation of the dates, including "backdating" if necessary, of the granting of stock options in such a way that the employee benefits from favorable movements in the stock price. This is commonly effectuated by choosing an option pricing date when the stock price was artificially low. When the grant or exercise price is less than the strike or the market price, the stock option is said to be "in the money." (Note: employees are always better off with in-the-money options, featuring the lowest exercise price possible.) Spring loading is the practice of granting options just before the release of good news that will send the stock prices higher. Bullet dodging is delaying the grant of options until bad news lowers the stock price.

28) Illegitimate off-balance sheet transactions: Transactions that are not accounted for in the company's financial statements. For instance, recognizing revenues and profits of another (unconsolidated) organization (that is, a related party) while at the same time dumping debts on that other organization's balance sheet. This gives the appearance of superior returns, with less debt.

29) False claims: The Federal False Claims Act permits a person with knowledge of fraud against the U.S. government, called a "qui tam plaintiff," to file a suit on behalf of the government against the business or person who defrauded the government (the defendant). If the action is successful, the qui tam plaintiff is rewarded with a percentage of the recovery.

30) Window dressing: Also called "apple polishing," this refers to the practice of making financial statement numbers look better than they are. When such presentation materially distorts the financial statement presentation, it becomes a type of cooking the books (see definition 3 above).

31) Channel stuffing: The business practice of inflating sales figures by dispatching more goods to a distribution channel than its capacity to sell. The sales manager may meet his or her earnings quota and bonus, but the goods from the overstuffed distribution channel are not sold and are returned to the organization, hurting it in the long run.

32) Insider trading: Using private, nonpublic information to trade in a company's shares to gain personal advantage and benefit. For example, company directors who become aware of poor product or project performance sell off their stock holdings before the stock price declines.

4. Fraud risk factors are latent variables — they constitute the underlying and frequently unobservable drivers of fraudulent, deceptive behavior. Fraud risk indicators are the patent or manifest variables — they are observable and thus can be traced back to the existence of associated underlying factors. Both fraud risk factors and indicators may differ by industry (for example, heavily regulated industries such as financial services and healthcare may have significant legal noncompliance risks) as well as geography (for example, perceptions of risk and fraud differ locally, regionally, nationally, and internationally). Furthermore, because not all fraud risks are created equal, they need to be prioritized in some manner such as impact and likelihood analysis. Such fraud risk analysis approaches require consideration of materiality (that is, the significance or importance to achieving organizational objectives), as well as the quality and quantity of evidence that needs to be gathered to gain reasonable assurance that the organization is protected from material fraud occurring (or knowing quickly when material fraud does occur). Following are some examples of fraud risk indicators arranged under each of the vertices of the fraud triangle: opportunity, pressure, and rationalization.

Opportunity (fraud risk indicators)

- Formal or informal restrictions on the auditors [both internal and outside auditors] that inappropriately limit their access to people or information, or that limit their ability to communicate effectively with the board or audit committee.
- Significant related-party transactions not in the ordinary course of business or with related entities that are not audited or are audited by another firm.
- Domination of management by a single person or a small group in a non-owner managed business without compensating controls.
- Ineffective accounting and information systems, including situations involving significant deficiencies or material weaknesses in controls.
- Inadequate monitoring of significant controls.
- Ineffective board or audit committee oversight over the financial reporting process and system of internal control system.
- High turnover rates or employment of unqualified accounting, internal audit, or information technology staff.

Pressure (fraud risk factors, adapted from SAS 99, AICPA)

- The organization's financial stability or profitability is threatened by economic, industry, or entity operating conditions such as:
  - High degree of competition or market saturation, accompanied by declining margins.
  - High vulnerability to rapid changes, such as changes in technology, product obsolescence, or interest rates.
  - Significant declines in customer demand and increasing business failures in either the industry or overall economy.
  - Operating losses making the threat of bankruptcy, foreclosure, or hostile takeover imminent.
  - Recurring negative cash flows from operations or an inability to generate cash flows from operations while reporting earnings and earnings growth.
  - Rapid growth or unusual profitability, especially compared to that of other companies in the same industry.
  - New accounting, statutory, or regulatory requirements.
- The organization's management is under excessive pressure to meet the requirements or expectations of third parties due to:
  - Profitability or trend-level expectations of investment analysts, institutional investors, significant creditors, or other external parties (particularly expectations that are unduly aggressive or unrealistic), including expectations created by management in, for example, overly optimistic press releases or annual report messages.
  - Need to obtain additional debt or equity financing to stay competitive, including financing of major research and development or capital expenditures.
  - Marginal ability to meet debt repayment or other debt covenant requirements.
  - Perceived or real effects of reporting poor financial results on significant pending transactions, such as business combinations or contract awards.
- The organization's management or the board of directors' personal net worth is threatened by the organization's financial performance arising from:
  - Heavy concentrations of compensation (for example, bonuses, stock options, and earn-out arrangements) being contingent upon achieving aggressive targets for stock price, operating results, financial position, or cash flow.
  - Personal guarantees of debts of the organization that are significant to their personal net worth.
- The organization's management or operating personnel are under excessive pressure to meet financial targets set up by the board of directors or management, such as sales or profitability incentive goals.

Attitude/Rationalization (fraud risk indicators)

- Significant, unique, or highly complex transactions, especially occurring close to year-end, that pose difficult "substance over form" questions.
- Domineering management behavior in dealing with the auditor, especially involving attempts to influence the scope of the auditor's work.
- Known history of violations of securities law, or claims against the organization, its senior management, or board members alleging fraud or violations of securities laws.

- Ineffective communication, implementation, support, or enforcement of the organization's values or ethical standards by management, or the communication of inappropriate values or ethical standards.
- Frequent disputes with the current or previous independent outside auditor on accounting, audit, or reporting matters.
- An interest by management in using inappropriate means to minimize reported earnings for tax-motivated reasons.
- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality.
- Management failure to connect known significant deficiencies or material weaknesses in controls in a timely manner.

Reference sources such as The IIA's *Standards*, along with the related Practice Advisories, International Standard on Auditing No. 240 from the International Federation of Accountants, Statement of Standards on Auditing (SAS) No. 99 from the AICPA, and the *Fraud Examiners Manual* from the ACFE, etc. provide a large amount of helpful materials to answer this question in depth.

5. Management override of controls is extraordinarily difficult to detect, especially because most internal auditors are trained to accept that "absence of evidence is evidence of absence." And when there is a motivated fraud perpetrator who is a member of senior management, he or she normally will go to great lengths to conceal evidence and cover up his or her tracks. Nevertheless, the internal audit function can be vigilant and take numerous steps to combat this disturbing possibility. For example:
   - Insisting on background checks for all employees before hiring, but especially for senior executives.
   - Maintaining an appropriate level of professional skepticism.
   - Working to educate the audit committee and building fraud awareness throughout the organization.
   - Brainstorming with the audit committee about potential fraud risks.
   - Leveraging the corporate code of conduct to assess the ethical temperature of the organization.
   - Nurturing operational risk management and compliance cultures.
   - Ensuring that the organization actively promotes and supports a whistleblower program, including a "no retaliation expectation."
   - Developing a broad information and communication feedback network.

   The internal audit function can serve as the "eyes and ears" of the audit committee by ensuring compliance with prescribed financial reporting controls. Whenever there is suspicion (for example, at quarter- or year-end) that management may have engaged in an override of controls to "manipulate or fudge the books," the internal audit function should inform the audit committee and secure the mandate to look into the possibility of fraudulent financial reporting. Similarly, through a series of interviews with employees, internal auditing can make appropriate inquiries about possible incidents of management override. If internal auditors are contacted by a whistleblower about the management propensity of control override, they should take such complaints seriously and keep the audit committee informed about follow-up activities that may be warranted in the circumstances. (Additional reference material pertinent to answering this question can be found in the AICPA's 2005 document, *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention.*)

6. Internal auditors have the training and experience to be viable parts of forensic investigations. It is important to assess whether they have the competence, independence, and objectivity to carry out such an investigation successfully. When the internal auditor finds the matter to be complex and beyond the scope of his or her expertise, he or she should recommend that a knowledgeable, suitably qualified forensic accountant or fraud examiner be engaged.

   When the internal audit function has been assigned an investigator's role, an investigation plan must be developed for each investigation, following the organization's investigation procedures or protocols. Any possibility that there might be a potential conflict of interest must be cleared. An investigation plan should consider methods to:
   - Gather evidence, such as surveillance, interviews, or written statements.
   - Document the evidence, considering legal rules of evidence and the business uses of the evidence.
   - Determine the extent of the fraud.
   - Determine the scheme (techniques used to perpetrate fraud).
   - Evaluate the cause.
   - Identify the perpetrators.

   At any point in this process, the investigator may conclude that the complaint or suspicion was unfounded and follow a process to close the case. Activities should be coordinated with management, legal counsel, and other specialists such as human resources and insurance risk management as appropriate throughout the course of the investigation. Investigators must be knowledgeable and cognizant of the rights of persons within the scope of the investigation and the reputation of the organization. The level and extent of complicity in the fraud throughout the organization should be assessed. This assessment can be critical to ensuring that crucial evidence is not destroyed or tainted, and to avoid obtaining misleading information from persons who may be involved. With respect to the involvement of the internal auditor in a fraud investigation, The IIA's *Standards* and related Practice Advisories are highly germane to the fraud investigation. In addition, the internal auditor also should be cognizant of all other applicable laws, regulations, and professional standards that bear upon his or her task.

7. Whenever a fraud allegation involves litigation, and the internal auditor gets involved in the investigation, it is prudent to seek the protection of attorney-client privilege. Otherwise, there is a significant possibility of adverse exposure to the internal auditor if their work is produced in court and challenged in a public forum. Litigation against the internal auditor may even arise.

CASES

Case 1

It is not clear from the case study whether Mr. Sam Rogers was a Certified Internal Auditor (CIA) or even a member of The IIA — such "professionalism" is a necessary but not a sufficient condition for performance in the discharge of the internal auditors' duties. If he was neither professionally certified, nor an IIA member, then serious doubts immediately get raised about the organizational status, independence, and objectivity of the internal audit function at Fannie Mae, including that of its chief audit executive (CAE). Mr. Rogers' fawning remarks about the CEO clearly suggest that he was beholden to, not independent of, the CEO, and was probably not in a good position to question or challenge the

undesirable "tone at the top" set by the (domineering) CEO. In this context, whenever the internal auditors' compensation includes stock options and bonuses tied to financial performance, it is easy to see that they end up having a vested interest in participating in fraudulent financial reporting for selfish gain. This is a form of "self dealing" that puts the internal auditors' personal interests ahead of the organization's and stakeholders' interests. Clearly, that would be a significant conflict of interest for an internal auditor — more so for the CAE — in an organization such as Fannie Mae.

Case 2

This case study is self-explanatory and answers will depend on the facts and circumstances of the fraud case studies chosen by each group of students. A good reference source with real-world case studies for external auditing is *Contemporary Auditing: Issues and Cases* by University of Oklahoma Professor M.C. Knapp (2004). The instructor may want to specify which fraud cases students should research.

Case 3

A. 1. "The **Benford** command allows [the auditor] to generate digital analysis using the Benford formula. This command counts the number of times each leading digit or digit combination occurs in a data set, and compares the actual count to the expected count. The expected count is calculated using the Benford formula. The command output can be sent to a graph."

   2. "Digital analysis tools like the Benford command enable auditors and other data analysts to focus on possible anomalies in large data sets. They do not prove that error or fraud exist, but identify items that deserve further study on statistical grounds. Digital analysis complements existing analytical tools and techniques, and should not be used in isolation from them."

   3. "Select **Analyze** from the menu bar and choose **Perform Benford Analysis** to display the **Benford** dialog box."

B. 1. "A **Benford's Law** analysis is most effective on data:
   - Comprised of similar sized values for similar phenomena.
   - Without built-in minimum and maximum values.
   - Without assigned numbers, such as bank account numbers and zip codes.
   - With four or more digits."

   2. The seven steps used to perform a Benford's Law analysis, as described in IDEA Help, are:
   - "Select **Analysis** > **Benford's Law** . . ."
   - "Select the field to analyze. In the **Field to analyze** drop-down list, select the Numeric field . . . to analyze with Benford's Law."
   - "Select the number type. In the **Include Values** area, select the check box for the required number type (**Positive** or **Negative**)."
   - "Optionally, specify the upper and lower boundaries. The **upper and lower boundaries** define the acceptable range of values where the actual result can appear. Select the **Show boundaries** check box to include the boundaries in the **Results** output and resultant database."
   - "Select the required analysis types. In the **Analysis Type** area, select the required **analysis types**, and then accept or change the associated database file names."

- "Optionally, create a **Results output**.
- Click **OK**.

3. When a Benford's Law analysis is performed, "The resultant database contains the following fields:
   - **DIGITS:** The digits that **Benford's Law** analyzes (1 through 9).
   - **EXPECTED:** The expected number of records with the listed digit in the place specified by the analysis type.
   - **LOWBOUND:** The low boundary number of records with the listed digit in the place specified by the analysis type.
   - **HIGHBOUND:** The high boundary number of records with the listed digit in the place specified by the analysis type.
   - **ACTUAL:** The actual number of records with the specified digit in the place specified by the analysis type.
   - **DIFFERENCE:** The number of records between the expected number and the actual number."

C. 1. "Payroll frauds are one of the most common types of fraud committed. Often a fictitious or "ghost" employee is set up on a salary system with payments following automatically. This is particularly true in the case of electronic payments into bank accounts where the cheques need to be collected. Other common ways to defraud a payroll system are by not removing leavers (terminations), then channeling their pay into another bank account, or by submitting excessive overtime, expense, or allowance claims."

2. "In most cases payroll frauds are found by accident, perhaps a query by the revenue authorities or a colleague who notices something suspicious. [Auditors] can use IDEA on a regular basis to analyze payments looking for unusual items, matching payments to the payroll master file ensuring correct rates, allowances, and deductions are applied, and identifying any "ghost" employees or duplicate payments."

3. Payroll "Tests [auditors] can carry out using IDEA include:
   - Duplicates.
     - Test for duplicate employees on the entire payroll file (appending or joining payroll files, if necessary) using the employees' Social Insurance, Social Security, or National Insurance Numbers as a unique employee identifier.
     - Check for duplicate bank accounts. This test may report family accounts where more than one member of a family is employed by the organization. However, these can be eliminated from the list of duplicates leaving the fraudulent items.
   - Cross-matches
     - Match master information from the payroll file with the organization's personnel file to determine whether there are "ghost" employees on the payroll.
     - Compare the payroll file at two dates, for example, the beginning and end of a month, to determine whether recorded starters and leavers (hires and terminations) are as expected and if any employees have received unusually large salary increases.
   - Exceptions
     - Ensure each employee's salary is between the minimum and maximum for his/her position or grade. [Auditors] should also test the reasonableness of allowances to position or grade.

CHAPTER 8
FRAUD RISKS & CONTROLS
Illustrative Solutions

   - Investigate excessive overtime and allowance claims to ensure there has been no over-claim.
   - Compare holidays and sick leave taken to the limits for a particular grade or position, and if there is a high rate of absenteeism or sickness, this could be analyzed by department to identify problem areas.
   - Evaluate the reasonableness of tax codes and compare changes in tax code over a period."