Fraud Detection for Government Auditors

Participant Guide

Welcome to The IIA Training Experience… Now What Happens?

- ✓ Welcome to your IIA on-site facilitated seminar. Throughout the duration of this event, your instructor will create an environment allowing you to participate in the learning process. Your instructor will provide the learning setting, engaging you in stimulating and thought-provoking discussions.

- ✓ Be sure to sign the sign-in sheet. You will be awarded CPE hours for your participation in this facilitated training session. Your CPE letter will be processed after your instructor returns the sign-in sheet. Please allow 2-3 weeks for receipt of your letter. You will receive your CPE letter from your training coordinator.

- ✓ Your feedback is important to us. Within 48 hours of the end of your event, your training coordinator will receive a link to the evaluation survey. Your training coordinator will forward that link to you and you will have two weeks to provide your feedback. We compile results and send the final report to your training coordinator and your instructor. While the survey does ask for your name, it ***does not*** attach it to your responses, assuring that your individual feedback will remain anonymous.

- ✓ How is your feedback used? Your training coordinator may use it in the decision-making process for future training. The IIA uses it in evaluating the quality of the course, materials, and instructor. The instructor will use your responses to improve upon their delivery methods.

- ✓ Never Stop Learning. Enjoy your training experience!

SCOTT LANGLINAIS, CPA

Scott Langlinais has dedicated the majority of his 20-year career as a CPA to fraud detection and investigation. Audit and finance professionals around the world have invited him in-house to educate their staff about proper fraud detection, prevention, and response. Business leaders from emerging companies to Fortune 500's, across many industries including public accounting, government, and not-for-profit, have asked him to assist with investigations, assess their environment, and design strategies to help defend the organization's people, reputation, and assets.

Mr. Langlinais employs IDEA® data analysis software to sift through system transactions and seek indicators of fraud, waste, and abuse. Using such techniques, he has helped companies recover millions of dollars from problems such as vendor overpayments, corruption, and unbilled revenues.

He speaks regularly at conferences hosted by the Institute of Internal Auditors, the American Institute of Certified Public Accountants, the Association of Certified Fraud Examiners, and the Information Systems Audit and Control Association. The International Risk Management Institute publishes his quarterly articles about fraud prevention.

Prior to starting his own practice in 2003, Mr. Langlinais held public accounting and internal audit leadership positions, most recently serving as Director of Internal Audit and Security for a NASDAQ 100 software company.
Mr. Langlinais serves as the Founder and Director of the Dallas Tax Assistance Program, a not-for-profit organization that assists low-income families with federal tax return preparation.

He received a BBA degree from the University of Notre Dame in 1991.

Welcome!

The role of belief

The challenge fraud presents

1.

2.

3.

Wal? Bal?

The Two Most Important Questions

1.

2.

More Challenges Presented by Fraud

Management expectations and the impact of beliefs

- Our people are honest, so we have no fraud
- Controls will prevent fraud
- Audits will detect fraud
- Good results, no surprises!

Management and auditors need to know:

- Emotional responses to fraud
- The most damaging kinds of fraud
- The Five Dangers!

Mishandling of investigation can lead to:

- Failure to file valid bonding claims
- Successful litigation by perpetrators or others
- Failure to identify all perpetrators
- Inability to terminate employment or contracts
- Failure to identify and correct control weaknesses
- Inability to report wrongdoing to law enforcement

Defining and Communicating Expectations
Related to Auditor Detection of Fraud

There may be no faster way to polarize auditors than to mention auditor responsibility for detection of suspected wrongdoing. Many public accountants, internal auditors and government auditors have something in common – they would prefer to disclaim accountability for detection. Yet the reason for the audit profession, at least the attest aspect, is to provide assurance that all is as stated… or not off by a material amount. Courts have consistently found that auditors have a responsibility for identification of material misstatements, particularly when they have ignored their own standards in the rush to please their clients or employers.

The real issue for auditors, including internal auditors, is to avoid being used as a scapegoat for management attempting to divert attention away from themselves. The following approach can help protect internal auditors from being unfairly blamed when fraud surfaces:

1. **Sponsor and implement a written fraud policy.** Policy should state that management is responsible for knowing exposures to fraud for their areas and for detecting suspected wrongdoing.
2. **Be involved in investigations, coordinating with legal.** Either take complete responsibility for investigations, or at a minimum determine the internal control implications of the case.
3. **Never say detection is not our job.** No one wants to hear that, least of all a CEO with a $40 million embezzlement. Auditors have program steps aimed at detection, including inventory observations, review of bank reconciliations and confirmations. If the warehouse is gone, the auditor is supposed to notice.
4. **Assume reasonable responsibility for some fraud detection.** Build fraud detection into routine audit activity and use data mining to bring fraud to the surface.
5. **Do an audit autopsy after a fraud.** Assess the effectiveness of the audit program steps and the performance of the staff. Auditors may need training or coaching… or they may need to leave. Lying about work, gross negligence, or willful blindness should result in consequences for the auditor!

We suggest telling executives and audit committees:

Knowledge of fraud exposures is required by audit standards.

1. *You can expect us to know fraud exposures for the areas we audit. If we don't know the exposures, we will seek to learn them.*
2. *You can expect us to know symptoms of fraud occurrence.*
3. *You can expect us to build tests to identify symptoms of fraud in routine audits.*
4. *You can expect us to use data mining or computer retrieval to identify symptoms.*
5. *You can expect us to follow up to determine fraud implications of any symptoms or exceptions identified in our audit work.*
6. *You can expect us never to hide or ignore symptoms of suspected wrongdoing.*

Defining & Communicating Investigative Responsibilities

Task or Objective	Client/ Management	Auditor/Accountant	Internal Investigator	Private Investigator	Law Enforcement	Attorney	Comments
A complete investigation:							
1. Determining whether fraud was committed							
2. Identifying the perpetrator							
3. Determining the method of operation							
4. Determining the internal control implications							
5. Determining the extent of the loss							
6. Documenting the case, for presentation to:							
Management							
Appropriate authorities							
Insurance carriers (Bonding company)							
7. Pursuing recovery							
8. Determining career implications for bosses							
9. Determining financial impact on statements, customer accounts and billings to third parties.							
Specific tasks:							
1. Determining the need for an investigation							
2. Planning the investigation							
3. Examining documents							
4. Gathering information about:							
Employees							
Vendors							
Customers							
Transactions							
Systems							
Accounts							
5. Using computers to detect fraud							
6. Using computers to analyze trends and patterns							
7. Determining what really happened							
8. Conducting Interrogative interviews							
9. Preparing case documentation							
10. Presenting case to law enforcement or prosecutors							
11. Seeking recovery of losses							
12. Advising management on career impact for bosses							

Assessing Fraud Policy

Is your fraud policy easily accessible? How is it communicated to the employees?

Is it known to all employees?

What evidence do we have that it is followed?

Is it complete? Does it cover each of the following?

A definition of unacceptable behavior, with examples.

- ✓ A list of redundant communication channels for reporting wrongdoing, accessible to all employees, vendors, and stakeholders.
- ✓ A statement that it is everyone's responsibility to help prevent unethical and illegal behavior.
- ✓ It is management's responsibility to understand *and detect* fraud, waste, and abuse in their own areas.
- ✓ A requirement that everyone must report wrongdoing when they see it.
- ✓ A clear identification of whose responsibility it is to investigate wrongdoing.
- ✓ A statement that all allegations will be investigated, and all results will be reported to the audit committee and the bonding company.
- ✓ Cover-up and retaliation against witnesses is forbidden.
- ✓ A requirement for employees to re-affirm the policy annually.

How would an auditor detect… ?

Exposure	Detection Method
1. The CFO claims there is inventory in warehouses that is not really there.	
2. The custodian of a bank vault took cash for herself. When a co-worker discovered the shortage, she persuaded her not to report the shortage, but instead participate in the theft. Over several years the two took $2.5 million from an $11.3 million fund.	
3. A car dealer who financed his inventory failed to reduce borrowing when cars were sold and removed from his dealership. He told auditors the vehicles were in transit.	
4. A telephone utility knowingly failed to bill the customer for telecommunications equipment and services.	
5. An executive arranged for a contractor to bill the company for work done on his home. The $2 million cost was buried in a $150 million project.	
6. An IT manager set her boyfriend up as a contractor and paid him $11 million over three years.	
7. Employees used company provided credit cards to entertain themselves and customers extravagantly and inappropriately.	
8. Bank loan officers made loans in excess of collateral in exchange for kickbacks and favors. When the loans became past due, the proceeds of new loans were recorded as payments on the past due loans.	
9. A sales representative arranged for customers to be billed for work not actually done. He sent the customers emails stating they did not have to pay the invoices.	
10. An accountant made journal entries to adjust accruals and revenue to make earnings targets.	

Introduction to Fraud Detection

Fraud surfaces through:

- Management review and other controls
- Internal audit
- Public accountants
- Law enforcement
- Regulators
- Concerned employees
- Outside informants
- Unsolicited confession

Opportunity for fraud to occur and go undetected is increased when:

- Segregation of duties breaks down.
- Segregation of duties is not practical.
- Supervisory review is absent or perfunctory.
- Controls break down!
    - Managers are ignorant of the exposures.
    - Managers are too trusting.
    - Managers are willfully blind to indicators of fraudulent activity.
    - Those responsible for control functions don't understand the fraud implications of their tasks.
    - Executives or others are blinded by prospects of profits, bonuses, or commissions.

17 Reasons Auditors Don't Detect Fraud

1. Too small
2. Not included in scope of work
3. They did not know exposures in specific terms.
4. They did not know symptoms of occurrence (how fraud is reflected in information)
5. They did not build program steps to identify specific symptoms of fraud occurrence.
6. They failed to follow through on symptoms observed because they:
    a. Failed to recognize them
    b. Were over concerned about budget
    c. Were afraid of career or client implications
7. They preferred to avoid conflict.
8. The situation was perceived as "too political"
9. They did not understand the population.
10. They did not understand how financial statements were prepared.
11. Inappropriate sampling approaches
12. Inadequate response to exceptions
13. They were fooled, compromised or intimidated.
14. Overly reliant on management representations
15. Lack of sufficient professional skepticism
16. Not ascertaining whether the financial statements agreed or reconciled with the accounting records
17. Not testing the accuracy of computer-prepared schedules

The Five Step Approach to Fraud Detection

1. Know the Exposures

2. Know the Symptoms of Occurrence

3. Be Alert for Symptoms & Behavior Indicators

4. Build Audit Programs to Look for Symptoms

5. Follow Through on All Symptoms Observed

Know the Exposures - Know what can go wrong. Know who could do it. Know what opportunities there are for employees, executives, outsiders, customers, licensees, agents, suppliers, contractors and others providing goods and services. For fraudulent financial reporting, know the pressure for favorable results. Understand the systems, the controls, and what they are intended to prevent or detect.

Know the Symptoms of Occurrence - Symptoms are specific. Symptoms may be of the fraud itself, or of the cover-up attempt. For each exposure know how it would be reflected in documents, reports, edits, computerized data, paid checks, reconciliations, accounts, complaint files, adjusting or correction entries.

Be Alert for Symptoms & Behavior Indicators - Many cases are detected by an auditor or manager following through on a symptom noted while actually looking for something else. Respond to identified behavior indicators and changes in patterns.

Build Audit Programs to Look for Symptoms - Determining exposures and evaluating internal control precedes writing the audit program. Some environments may lack controls that the internal auditor can rely upon to protect his organization's interests. Such environments include some branch offices and other remote locations, and outsiders such as vendors, agents and contractors. Even in the organization with good controls, frequently there are areas or departments lacking segregation of duties or meaningful supervisory review.

In developing the audit program the internal auditor should include specific steps designed to look for symptoms of fraud. Sampling plans should take into consideration the fraud exposure and the reliability of internal controls.

Building audit programs to look for symptoms includes:

- Brainstorming fraud exposures for each audit.
- Identifying symptoms of fraud occurrence for each exposure.
- Developing symptom-specific program steps.

Five Step Approach
(continued)

In addition, auditors wanting to detect fraud can:

- Select judgmental samples based upon knowledge of symptoms.
- Use computer techniques to look for fraud occurrence.

Stratification of the population, stratified sampling, directed sampling, and discovery sampling may prove to be helpful. In the completely uncontrolled environment the auditor will want to determine the tolerable undetected fraud allowable in the population. The auditor may want to design the sample so as to include a fraudulent occurrence should the level of fraud in the population aggregate more than the tolerable amount.

Note: *No fraud is acceptable, but auditors in deciding sample sizes actually are determining the probability of having **the opportunity** to detect fraud. The probability is dependent upon the amount of fraud, the size of the population and the sample selected.*

Follow Through on All Symptoms Observed - The auditor should resolve all symptoms. The auditor should operate with an attitude of healthy professional skepticism. Beware of pressures to complete work on time. The single symptom you are looking at may not be an isolated occurrence; **it may be one of many**.

Auditors should assess the fraud implications of all exceptions noted. Resist the temptation to explain an exception as an isolated incident or immaterial.

Remember
"It's immaterial" should not be applied to explain an exception in a sample!

Complete the following to reflect resolution of fraud implications of exceptions:

Potential Fraud

Exception	*Perpetrator*	*Fraud Act*	*Benefit*[1]	*Victim*[2]	*Action*[3]

[1] ***Benefit:*** *Sometimes the benefit is obvious, as in an embezzlement. Sometimes it is more subtle, as in claiming deliveries were short to hide missing inventory.*

[2] ***Victim:*** *Sometimes the organization is the victim, while other times the victim is a customer, an employee, a vendor or a taxing authority.*

[3] ***Action:*** *If, in completing this worksheet, the auditor is able to determine that the exception is indicative of a potential fraud, then **Action** steps should be taken to determine whether fraud did occur. If, in completing the worksheet, the auditor is unable to identify any potential fraud, perhaps no further work is needed.*

What Can Go Wrong

In Government Entities

1. A firefighter with a $40,000 salary cleared $160,000 in income for the year due to false overtime.

2. Government logistics contractors supplying an army overseas falsified their returns and scuttled empty ships to claim massive compensation for loss in storms.

3. A local government official waived fines in exchange for a fee.

4. An accountant manipulated formulas in a spreadsheet of account adjustments in hopes that the auditors would not recalculate all of the rows and columns.

5. A technology firm under the Federal E-rate program paid bribes and kickbacks to school officials to bypass the competitive bid process and award the contract to the firm.

6. A city mayor used holiday gift cards for personal purchases. The gift cards were to be distributed to needy families.

7. A small parts supplier collected $20 million over five years from the Pentagon for fraudulent shipping costs, including $998,798 for sending two 19-cent washers to an army base in Texas.

8. The Director of Internal Audit of a school district made himself the sole signatory on a bank account in the name of a charter school and embezzled public funds.

9. A vendor invoiced an organization twice for the same leased product. Because the vendor had leased dozens of the product to the customer, the vendor knew the customer would be unlikely to notice. The vendor over billed $1 million in one year.

10. A local official circumvented his approval limit by asking the vendor to split the invoices for a single purchase.

11. An A/P clerk knew that no one reviewed invoices under $500. She directed her husband to send the organization numerous $490 invoices which she entered into the system and buried in a cost center with a huge budget.

12. An approving official authorized an overpayment to a vendor and agreed to split the difference. The official deleted the check from the system and covered up the reconciling item.

13. An IT director with responsibility for purchasing network hardware established a shell company to purchase the equipment from a legitimate vendor. He marked up the equipment

and used his authority to purchase the equipment from the shell company at the marked up rate. The total loss exceeded $5 million.

14. A vendor learned a customer's tolerance limit for the amount in which invoices could exceed the purchase order without being subject to review. Upon billing their products, they slightly increased the price of every item above the contract price to fall within the tolerance thereby gaining an extra $10 million.

15. A manager with a $10,000 approval limit asked procurement to set up a vendor in the system. She fabricated purchase orders and had a friend mail false invoices from the vendor name for amounts just under her approval limit.

16. The travel team failed to review the travel system for employees who purchased a refundable, full-fare plane ticket but never took the flight. The result was $700,000 in unused plane tickets, many of which were cashed in by the employees.

17. A director submitted travel expenses three times for reimbursement: once with a legitimate expense report, a second time with the receipts photocopied, and a third time with the credit card statements of the expenses he already submitted.

18. An official purchased expensive one-way, full fare airline tickets and submitted them for reimbursement. He would then get a refund for the ticket, fly to his destination on a low-fare ticket, and keep the difference.

19. Seventy-four government-issued credit cards distributed among 13 employees included $5.9 million in personal charges. An anonymous letter tipped off the fraud.

20. Over a two-year period one administrative assistant of a school district spent $383,788 on her government-paid credit card but had no receipts to support her purchases.

21. A pharmaceutical company misreported several of its "branded" drugs as "generic" to reduce its quarterly rebate obligation under the Medicaid Prescription Drug Rebate Program. The company underpaid rebates by over $10 million.

22. A family practice doctor based in a low-income neighborhood prescribed medication that made patients ill so they would return for a follow-up visit. He billed Medicaid for the visits.

23. An official skimmed revenues and sent the money to an off-shore bank account. Those revenues were not recorded in the books.

24. An airport security company underreported revenues to the county to avoid paying permit fees based on gross revenues. Loss to the county was $200,000.

25. A collector posted credit memos to outstanding balances in exchange for kickbacks or simply to provide free goods and services to friends and family.

26. An employee intercepted customer payments and covered up the theft with a false entry in revenues. The original documents were destroyed.

27. A warehouse employee stole product and agreed to split it with someone in accounting if they would book a false receivable. The accountant agreed and wrote off the receivable to bad debts immediately, posted an unauthorized credit memo to the receivable, or allowed the receivable to age and be written off naturally after 120 days.

28. An official with system access pushed forward the due date on fines or penalties so the amount never became past due.

29. A payroll manager left terminated employees in the payroll system and re-directed the payments to her own bank account.

30. A manager created a fictitious employee file with his wife's personal and bank account information, and treated this 'employee' as a new-hire. Payroll set up the information in the system and unknowingly placed the manager's wife on the payroll.

31. A benefactor donated $1 million to a university. In exchange, the institution put the benefactor on the payroll with a $100,000 annual salary even though the benefactor performed no work for the university.

32. When a pensioner died, the benefits administrator did not remove them from the system. Instead the administrator re-directed their pension payments to a PO Box where he collected the checks, falsified the endorsement and cashed them. The amount collected was $2.1 million.

33. An administrative assistant who input time cards into the payroll system agreed to falsify time worked in exchange for a cut of the overtime.

34. A group of contractors billed an average of 50 hours per week, including Thanksgiving and Christmas holidays, despite working less than 40 on average. In six months, the over-billing totaled $240,000.

35. Law enforcement officials used fleet vehicles to take their families on vacation.

36. A shipper took extra inventory and worked out a deal to split the goods with the warehouse manager if he would falsify the count sheets.

37. An official stealing inventory from government offices fooled the auditors by explaining the missing items are "inventory in transit." The auditors failed to notice the in-transit figure had grown every year and exceeded $1 million.

38. An official ordered excess computers and stacked them under a tarp in a corner of the office because he did not want to lose his budget.

39. Over four years a government agency paid $291,000 to an air conditioning vendor for overcharges, replacement costs covered by warranties, installations that did not occur, and one missing unit. The overcharges resulted from the vendor invoicing for more expensive units than were actually installed.

40. A cafeteria employee with a catering business on the side instructed the food vendor to drop off extra product at her home. The government's food service was billed for the full delivery.

41. A food stamp recipient filed for benefits at multiple offices. She submitted different names for herself at the different offices but submitted her children's names and dates of birth accurately.

42. A school superintendent purchased land for himself using $100,000 in school funds. A board member's signature stamp was used to approve board minutes which approved the purchase, although the board member was not present at the meeting. The board members present did not realize the land was being purchased for personal use.

43. University administrators credited 100 students' accounts just under $200,000 in a debt forgiveness program that had no eligibility criteria.

Cash Receipts

1. A salesman collected from a customer and never turned in the cash or the order.

2. A retail clerk received payments, failed to record the sale, and pocketed the proceeds.

3. A bartender recorded less than the proceeds of a transaction and pocketed the difference.

4. The accounts receivable clerk stole payments on account. The clerk covered it up by lapping payments from other accounts.

5. A retail clerk scanned only one of three items purchased, charged the customer for three items and pocketed the difference.

6. The accounts receivable clerk stole payments on account. The clerk covered it up by adjusting the customer's account for the amount of the payment.

7. The accounts receivable clerk stole payments on account. The loss was covered up by making a fictitious deposit in transit.

8. The accounts receivable clerk stole payments on account. The loss was covered up by debiting an expense account or any account not frequently scrutinized, such as suspense accounts, intercompany accounts, past due receivables.

9. Money was removed from the bank deposit after it was prepared. It was short when received at the bank.

Accounts Payable or Cash Disbursements

1. An accounting supervisor set up a fictitious payment scheme. A vendor number was obtained, and bogus invoices for services never rendered were paid. Checks were sent to a P.O. Box or to the home of the accounting supervisor.

2. A vendor accidentally billed the company twice for goods or services provided. When the payment was received and nobody noticed, the vendor began sending duplicate billings intentionally.

3. A vendor advised an accounts payable supervisor that they had been overpaid. The supervisor requested that the repayment be directed to his attention so that proper credit could be made. The supervisor converted the payment to his own use. He then began making duplicate payments on purpose, requesting repayment, and converting them.

4. An unknown outsider printed copies of company checks and ran them through the bank account. The company was unable to recover the $150,000 through banking channels since they were behind on their reconciliations.

5. Employees inflated their travel expense reports by:

    a. Altering restaurant receipts
    b. Making fictitious receipts by scanning in real receipts and altering them
    c. Submitting receipts and later submitting charge tickets
    d. Submitting personal receipts, claiming they were business expenditures
    e. Submitting airline tickets for trips never taken
    f. Buying high cost tickets, using the receipt for reimbursement, getting a refund and buying a discounted ticket for travel
    g. Getting reimbursed for receipts for purchased tickets, but using frequent flyer award tickets for business travel, then getting a refund for the unused purchased ticket
    h. Submitting receipts for limo service reimbursements that were also direct billed to the company
    i. Claiming mileage driven in excess of actual
    j. Claiming mileage although they rode with another employee
    k. Getting reimbursed for trips that had no business purpose

6. An employee bought postage stamps and was reimbursed through an expense report. He altered the amount after the boss approved the report. The boss increased the budget for postage. The documented loss exceeded $175,000.

7. The employee responsible for refilling the postage meter took a check for $5,000 to the post office, had $4,500 in postage placed in the meter and got $500 in stamps, which he sold.

8. An accountant processed fictitious claims for unclaimed funds waiting to be escheated to the state.

9. An accountant processed unauthorized telephone transfers to his own account and to pay personal vendors.

10. A treasury services employee processed unauthorized wire transfers for his own benefit. The loss exceeded $3 million and took place over two years.

11. A bank trust department diverted over $15 million in dormant customer pension trust accounts to the bank in order to increase bank profits.

12. An employee changed the address on suspended (dormant) accounts and then filed fictitious claims to obtain the funds.

13. A boss gave his administrative assistant his password so she could approve his subordinates' travel expenses on line when the boss was not available. The administrative assistant set up fictitious expense reimbursements for herself and used the password to approve them as well. She surmised that the manager might use the same password to approve payments to vendors. She made fictitious payments to fictitious payees using the same password.

14. The petty cash custodian in a trucking operation ran dummy receipts through the petty cash reimbursement. The loss exceeded $200,000.

Purchasing

1. An employee gave business to a favored vendor in exchange for a commission, sexual favors and free vacations.

2. A vendor compromised a purchasing agent by sending gifts to the agent's home. The purchasing agent sided with the vendor when he charged excessive prices or delivered shoddy merchandise.

3. Vendors got together to rig bids. When one of them got the work at a higher price, the others became subcontractors to the winner.

4. A manager with authority to select vendors solicited business from a particular vendor in exchange for stock in the vendor. The rationale was to reduce the charge from "kickbacks" to "conflict of interest."

5. A vendor gave a financial services company's purchasing agent a credit card for gasoline and other purchases.

6. Employees used procurement cards for personal purchases, inappropriate entertainment, and

cash advances for personal use.

7. A car dealer provided cars to the company fleet manager and his family each year to "try out."

8. A purchasing agent makes sure his "partner" gets the bid by:

    a. Telling him the bids by others
    b. Throwing away low bids by others
    c. Making up reasons not to accept low bids by others
    d. Not providing all bidders all pertinent information
    e. Sending out requests for bids too late for responses
    f. Structuring specifications so only favored bidder can win

9. A regional manager for a retail convenience store and gas station chain became disenchanted with the company. In anticipation of leaving, he went into business for himself, and built his own new store in a prime location. All of the construction costs, store fixtures and initial inventory were paid for by the company, which was also building new stores in the area.

10. A defense contractor substituted materials he claimed were "just as good," as those specified in the contract. To avoid detection, he manufactured labels to appear the same as those specified.

11. A project manager responsible for building offices arranged for the contractor to do work on his own house. The cost of the improvements was billed to the company.

12. Company executives responsible for negotiating leases for retail and office space acquired property just prior to leasing it to the company. Rental rates were excessive and the duration of the leases were longer than normal.

13. A telecommunications manager arranged for a long distance contract at a favorable rate. When the vendor billed the charges at $.02 per minute more than the contract, he approved the invoices in exchange for a kickback.

14. A law firm billed for hours not worked, sometimes billing as many as 40 hours in one day.

15. A consulting firm billed at the hourly rate of the partner even though the work was actually done by an entry-level staff associate.

16. A consulting firm claimed that a computer system would do things they knew the system could not do. When clients complained the consultants offered the services as enhancements to the system.

Payroll & Employee Reimbursements

1. A payroll clerk duplicated travel allowances, submitted the legitimate one to the actual employee, and a second, identical in every way except the dollar amount, was directed to his own bank account. Over eight years the clerk directed $21 million in payroll funds to his own bank account.

2. When a pensioner died, the benefits administrator would not remove them from the system, but rather would re-direct their pension payments to a PO Box where the administrator could collect them, falsify the endorsement, and cash them. The amount collected was $2.1 million.

3. An administrative assistant at a college who input time cards into the payroll system agreed to falsify time worked in exchange for a cut of the overtime. Ten college students became convicted felons before their careers began, and the total theft amounted to over $250,000.

4. Shortly after an organization implemented a purchase card program, it was discovered that 74 credit cards were distributed amongst three employees plus ten of their friends and family. These 13 people spent $5.9 million on personal items, reimbursed by the organization.

5. A school superintendent and his wife charged $640,000 in personal expenses to his district-paid procurement card. In another major district, one administrative employee amassed $330,000 personal expenses in one year, another $275,000.

6. The travel team failed to review the system for employees who purchased a refundable, full-fare plane ticket but never took the flight. The result was $700,000 in unused plane tickets. In many of these cases, the employees received a refund for the unused ticket and also received a reimbursement on their expense report.

7. Two hourly employees agreed to collude for the purpose of receiving overtime pay for time not worked. One arrived early and clocked in for both. The other left late and clocked out for both. Over several months each employee was paid for hundreds of overtime hours not worked.

8. A group of contractors billed an average of 50 hours per week, including over the Thanksgiving and Christmas holidays, despite working less than 40 on average. In six months, the over-billing totaled $240,000.

9. A benefactor donated $1 million to the institution. In exchange, the institution put the benefactor on the payroll with a $100,000 salary even though the benefactor provided no service and was not employed by the institution.

10. A salesman received two commissions for a $6 million sale, resulting in an overpayment of $300,000.

11. A payroll manager left terminated employees in the payroll system and re-directed the payments to his own bank account.

12. Undocumented immigrants received social security cards on the black market, and used these false social security numbers when completing their human resources documents.

13. A manager created a fictitious employee file with his wife's personal bank account information, and treated this 'employee' as a new-hire, even though she did not work for the company. Payroll set up the information in the system and unknowingly placed the manager's wife on the payroll.

14. An employee with update access to the Payroll Master File colluded with several employees to increase their wages / benefits received in exchange for a cut of the funds received. Alternatively, the employee with system access provided themselves an unauthorized raise.

15. A purchasing director submitted his travel expenses three times for reimbursement: once with a legitimate expense report, a second time with the receipts photocopied, and a third time with the credit card statements of the expenses he already submitted.

16. An executive assistant had full access to the CFO's credit card, and she received his monthly statements. Neither the CFO nor anyone else reviewed the statements. She and her husband were able to charge $100,000 in personal expenses to his company-paid card.

17. A general manager cut off their employees' ability to use their company-paid credit cards on Sundays. Annual purchases subsequently decreased by $200,000.

Symptoms of Fraud Occurrence

Understanding symptoms of fraud is the key to the detection of wrongdoing. A symptom of fraud may be defined as a condition that is directly attributable to dishonest or fraudulent activity. It may result from the fraud itself or from the attempt to conceal the fraud.

Managers and auditors interested in operating controls need to be familiar with what can go wrong in the areas they manage or audit. And they need to know what symptoms may be reflected in books, records, accounts, documents, reports and reconciliations if something does go wrong. Knowledge of exposures and symptoms is needed by anyone working with controls.

Examples of symptoms of fraud include:

1. Missing documentation
2. Denial of access to records
3. Shortages or overages in cash drawers
4. A bank deposit includes a check that is not rung on a cash register tape, recorded on a transaction log, or included in transactions for the day
5. Control total of checks received does not balance to checks deposited
6. Presence of a "thief's adding machine"
7. Excessive voids or refunds
8. Common names or addresses for refunds
9. Deposits in transit are slow in reaching the bank
10. Deposits in transit are growing
11. Manual or computer detail does not equal control totals
12. General ledger does not balance
13. Customers complain, "I paid this!"
14. Adjustments to receivables
15. Increases in past due accounts
16. Excessive late charges

Symptoms:

17. Increase in write-offs of late charges
18. No collections on past due or written off accounts
19. Adjusting entries lack formal approval
20. Shortages in inventory
21. Adjustments to inventory
22. Deviation from specifications on delivered goods or services
23. Shortages on delivery
24. Check amounts have been altered
25. Goods purchased are in excess of needs
26. Delivery location is not your office, plant or job site
27. Duplicate payments
28. Employees are not present at the payroll payoff
29. Payroll checks have second endorsements
30. Payroll checks have second endorsements by a boss
31. Handwriting on endorsements does not match signatures on file
32. Multiple employees use the same bank account numbers for direct deposit
33. Invoices are duplicates or copies
34. Invoices from consultants or contractors are handwritten
35. Old outstanding checks in bank reconciliations
36. Payees have common names and addresses
37. Address change followed by a request for payment
38. Activation of a dormant account, followed by a payment

Symptoms:

39. Vendor's address is the same as an employee address
40. Employees make entries or adjustments to their own accounts
41. Top performance by a new salesperson
42. Any performance that is too good to be believed
43. Alterations of documents
44. Changes in logs, daybooks, time reports
45. Liquid paper, erasures or other alterations on timecards
46. Copies where originals are expected
47. Support for payments is not cancelled or marked paid
48. An employee name or number is coded into an application program
49. A computer report total is incorrect
50. Math errors in spreadsheets
51. An employee does not remember working on a job his hours were charged to
52. Payments made in currency when checks were expected
53. Account details (bank, inventory, receivables) are not reconciled to the general ledger
54. Unlocated differences in reconciliations
55. Cost overruns on projects
56. Barely making goals
57. Auditees falsify documents to avoid audit findings
58. A vendor invoice is not folded when you expect it would be
59. Missing first milestone
60. Anything strange, odd & curious

Brainstorming Fraud Exposures

AREA	PERPETRATOR	FRAUD ACT

Relating Exposures to Symptom Driven Program Steps

SYMPTOM OF FRAUD OCCURRENCE	SYMPTOM DRIVEN AUDIT PROGRAM STEP TO DETECT
1.	
2.	
3.	