Study Notes

Specialization
MODULE-6
SP-612

Fraud Investigation and Audit

ICPAP
Institute of Certified Public Accountants of Pakistan

Question No 1. Explain Classic Fraud Research Theories.

Classic Fraud Research

Fraud is a topic much in vogue today. Seminars, symposia, and conferences on that subject abound, sponsored by government agencies, universities, trade groups, professional organizations, chambers of commerce; and business, fraternal, and religious organizations. Most are well attended, particularly because the cost of such crimes to individual businesses and society is substantial, but also because few know much about fraud. Reviewing the literature creates an appreciation for the scope and nature of fraud and builds a foundation for understanding fraud topics. The current term fraud was traditionally referred to as white-collar crime, and the two are used synonymously here. The classic works on fraud are White Collar Crime, by Edwin H. Sutherland; Other People'sMone, by Donald R. Cressey; The Thief in the White Collar, byNorman Jaspan and Hillel Black; and Crime, Law, and Society, byFrank E. Hartung.

These authorities essentially tell us:

White-collar crime has its genesis in the same general process as other criminal behavior; namely, differential association. The hypothesis of differential association is that criminal behavior is learned in association with those who define such behavior favor-ably and in isolation from those who define it unfavorably, and that a person in an appropriate situation engages in such criminal behavior if, and only if, the weight of the favorable definitions exceeds the weight of the unfavorable definitions.

In other words, birds of a feather flock together, or at least rein-force one another's rationalized views and values. But people make their own decisions and, even if subconsciously, in a cost-benefit manner. In order to commit fraud, a rationalization must exist for the individual to decide fraud is worth committing.

Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non shareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply their own con-duct in that situation, verbalizations which enable them to adjust their conceptions of themselves as users of the entrusted funds or property.

Jaspan tried to derive antifraud measures in his research. His book, The Thief in the White Collar, is based on his many years of consulting experience on security-related matters, and contains a number of notable and often quoted generalizations. In a nutshell, Jaspan exhorts employers to (1) pay their employees fairly, (2) treat their employees decently, and (3) listen to their employees' problems, if they want to avoid employee fraud, theft, and embezzlement. Butto temper that bit of humanism with a little reality, he also suggests that employers ought never to place full trust in either their employees or the security personnel they hire to check on employees.

Jaspan, like P. T. Barnum, would always cut the deck. Hartung disagrees with Jaspan's generalizations and focuses on the individual. He argues:

It will be noticed that the criminal violator of financial trust and the career delinquent have one thing in common: Their criminality is learned in the process of symbolic communication, dependent upon cultural sources of patterns of thought and action, and for systems of values and vocabularies of motives.

In reality, both Jaspan and Hartung appear to have been correct. Hartung noted that individuals are inevitably affected by their environment. Although Jaspan might be considered too empathetic to the individual, his suggestions to deter fraud echo the same as modern efforts do: Create an environment with few reasons and with few opportunities to commit fraud.

Question No 2. Fraud Triangle is considered essential in Anti-Fraud Field. How Fraud Triangle help investigators in understanding criminal behaviors'?

Why Is Fraud Committed?

Fraud or intentional deception is a strategy to achieve a personal or organizational goal or to satisfy a human need. However, a goal or need can be satisfied by honest means as well as by dishonest means. So what precipitates, inspires, or motivates one to select dishonest rather than honest means to satisfy goals and needs? Generally speaking, competitive survival can be a motive for both honest and dishonest behavior. A threat to survival may cause one to choose either dishonest or honest means. When competition is keen and predatory, dishonesty can be rationalized quickly. Deceit, therefore, can become a weapon in any contest for survival. Stated differently, the struggle to survive (economically, socially, or politically) often generates deceitful behavior. The same is true of fraud in business.

"Fraud Triangle"

Of the traditional fraud research, Donald Cressey's research in the1950s provides the most valuable insight into the question why fraud is committed. The result of this research is most commonly, and succinctly, presented in what is known as the fraud triangle. Cressey decided to interview fraudsters who were convicted of embezzlement. He interviewed about 200 embezzlers in prison. One of the major conclusions of his efforts was that every fraud had three things in common:

(1) Pressure (sometimes referred to as motivation, and usually an "unshared able need");

(2) Rationalization (of personal ethics); and

(3) Knowledge and opportunity to commit the crime.

Pressure (or incentive, or motivation)

It refers to something that has happened in the fraudster's personal life that creates a stressful need for funds, and thus motivates him to steal. Usually that motivation centers on some financial strain, but it could be the symptom of other types of pressures. For example, a drug habit or gambling habit could create great financial need in order to sustain the habit and thus

create the pressure associated with this aspect of the fraud triangle. Sometimes a fraudster finds motivation in some incentive. For instance, almost all financial statement frauds were motivated by some incentive, usually related to stock prices or performance bonuses or both. Sometimes an insatiable greed causes relatively wealthy people to commit frauds.

Beyond the realm of competitive and economic survival, what other motives precipitate fraud? Social and political survival provides incentives, too, in the form of egocentric and ideological motives, especially in financial statement frauds. Sometimes people commit fraud (deception) to aggrandize their egos, put on airs, or assume false status. Sometimes they deceive to survive politically, or have a burning desire for power. They lie about their personal views or pre-tend to believe when they do not. Or they simply cheat or lie to their political opponents or intentionally misstate their opponents' positions on issues. They commit dirty tricks against opponents. Motives to commit fraud in business usually are rationalized by the old saying that all is fair in love and war—and in business, which is amoral, anyway. There is one further category of motivation, how-ever. We call it psychotic, because it cannot be explained in terms of rational behavior. In this category are the pathological liar, the professional confidence man, and the kleptomaniac.

Rationalization

Most fraudsters do not have a criminal record. In the ACFE Report to the Nation (RTTN) 2004, 88% of the reported fraudsters had no prior criminal record. In fact, white-collar criminals usually have a personal code of ethics. It is not uncommon for a fraudster to be religious. So how do fraudsters justify actions that are objectively criminal? They simply justify their crime under their circumstances. For instance, many will steal from employers but men-tally convince themselves that they will repay it (i.e., "I am just borrowing the money"). Others believe no one is hurt so that makes the theft benign. Still others believe they deserve a raise or better treatment and are simply taking matters into their own hands to administer fair treatment. Many other excuses could serve as a rationalization, including some benevolent ones where the fraudster does not actually keep the stolen funds or assets but uses them for social purposes (e.g., to fund an animal clinic for strays.

Opportunity

According to Cressey's research (i.e., the Fraud Tringle), fraudsters always had the knowledge and opportunity to commit the fraud. The former is reflected in known frauds, and in research studies such as the ACFE RTTNs, that show employees and managers tend to have a long tenure with a company when they commit the fraud. A simple explanation is that employees and managers who have been around for years know quite well where the weaknesses are in the internal controls and have gained sufficient knowledge of how to commit the crime successfully. But the main factor in opportunity is internal controls. A weakness in or absence of internal controls provides the opportunity for fraudsters to commit their crimes. It is noteworthy that the Tread way Commission (later known as the Committee of Sponsoring Organizations, or COSO) was formed to respond to the savings and loan frauds and scandals of the early 1980s. The committee's conclusion was that the best prevention was strong internal controls, and the result was the COSO model of internal controls. On-the-job fraud, theft, and embezzlement are products of motivation and opportunity.

The motivation may be economic need or greed, egocentricity, ideological conflicts, and psychosis. Most on-the-job frauds are committed for economic reasons and often are attributable to alcoholism, drug abuse, gambling, and high lifestyle .Loose or lax controls and a work environment that does not value honesty can provide the opportunity. Motivations and opportunities are interactive: The greater the economic need, the less weakness in internal controls is needed to accomplish the fraud. The greater the weakness in controls, the level of motivational need necessary to commit a fraud is less.

Question No 4. Discuss the scope of Fraud.

Scope of Fraud:

How pervasive is business fraud? How likely is it to be discovered either by audit design or by accident? Research in the last 10 years has been able to reveal both the scope of fraud and the most effective means of detecting frauds. The scope of fraud is such that almost all midsize to large businesses are certain to have a fraud currently being or soon to be perpetrated. Virtually no small business is safe. Nor are not-for-profits or other types of organizations. Research by the

ACFE reveals that the estimated level of fraud detected from 1996 to 2004 has been consistent in the U.S. economy—approximately 6% of annual revenues.

Regarding financial frauds, a major study by COSO provides valuable insights. In 1998, COSO released its Landmark Study on Fraud in Financial Reporting

The report covered 10 years of the Securities and Exchange Commission (SEC) enforcement cases, analyzing 200 randomly selected cases of alleged financial fraud investigated by the SEC—about two-thirds of the 300 SEC probes into fraud between 1987 and 1997. COSO examined certain key company and management characteristics, and the key findings were interesting: Most fraud among public companies was committed by small firms (well below $100 million in assets), boards of directors were dominated by insiders and inexperienced people, executive officers were identified as associated with financial statement fraud in83% of the cases, and the average fraud period extended over a period of 23.7 months. The report went on to say: "The relatively small size of fraud companies suggests that the inability or even Unwillingness to implement cost-effective internal controls may be a factor affecting the likelihood of financial statement fraud." COSO suggested external auditors focus on the "tone at the top" in evaluating internal control structures.

In 2003, KPMG released its third Fraud Survey In it, KPMG surveyed 459 public companies and government agencies. The report found that fraud is increasing in the number of instances reported since its last survey. Of the respondents, 75% reported losses due to fraud in 2003, as compared to 62% in 1998. Employee fraud was most common category of fraud (60%). The category of financial reporting frauds averaged $257.9 million in costs per organization for the previous year, and the category of medical/insurance frauds averaged $33.7 million. These were the most costly fraud categories in the survey. Of the frauds reported, 36% incurred $1 million or more in costs, up from 21% in 1998. The median loss per incident was $116,000 for all types of fraud (1998). Only 4% of the frauds were discovered during financial statement audits in the 1998 survey, up to 12% in 2003. The most frequent methods of detection were internal controls (77%), internal audit (66%), employee tip (63%), and accident (54%). Obviously, there was some overlap in multiple detection methods. The ACFE tracks the trend in fraud and statistics on fraud regularly. It has been conducting surveys on occupational fraud and abuse since 1996 and

communicating the results to the public via its Report to the Nation. In all three reports (1996, 2002, 2004), the ACFE surveyed hundreds of Certified Fraud Examiners (CFEs), who reported facts on a fraud from the previous year. The results show enormous amounts of fraud each survey. The reported losses due to fraud were about 6% of reported revenues for those entities for each of the three years. Thus one measure of the scope of fraud is about6% of the U.S. economy, or about 6% of the average firm. According to the most recent ACFE RTTN (2004), that figure would be $660 billion total. Fraud losses have increased by 50% since the first survey in 1996. Financial frauds lasted an average of 25 months before being discovered.

The various ACFE RTTNs have also measured the common methods of detecting fraud. According to the reports, tips and com-plaints have consistently been the most effective means of detecting frauds, and are a much higher percentage than the second most effective means. Tips and complaints accounted for 39.6% of the initial detection of occupational fraud in the 2004 report. Internal audit was second (23.8%), accident was third (21.3%), internal controls was fourth (18.4%), and external audit was fifth (10.9%).

These research studies and other similar research show that fraud, of various kinds, is widespread. The best detection methods include tips, internal controls, and internal audit. The first two are integral tenets of the Sarbanes-Oxley Act of 2002.

Question No 5. Criminal minds become fraudsters if they play intelligently. What you mean by fraudsters profile?

Who Commits Fraud?

In view of the last section, one might conclude that fraud is caused mainly by factors external to the individual: economic, competitive, social, and political factors, and poor controls. But how about the individual? Are some people more prone to commit fraud than others? And if so, is that a more serious cause of fraud than the external and internal environmental factors we have talked about? Data from criminology and sociology seem to suggest so. Let us begin by making a few generalizations about people.

- Some people are honest all of the time.

- Some people (fewer than the above) are dishonest all of the time.
- Most people are honest some of the time.

Some people are honest most of the time. Research has been conducted to ask employees whether they are honest at work or not. Forty percent say they would not steal, 30%said they would, and 30% said they might. Beyond those generalizations about people, what can we say about fraud perpetrators? Gwynn Nettle, in Lying, Cheating and Stealing, offers these insights on cheaters and deceivers:

- ✓ People who have experienced failure are more likely to cheat.
- ✓ People who are disliked and who dislike themselves tend to be more deceitful.
- ✓ People who are impulsive, distractible, and unable to postpone gratification are more likely to engage in deceitful crimes.
- ✓ People who have a conscience (fear of apprehension and punishment) are more resistant to the temptation to deceive.
- ✓ Intelligent people tend to be more honest than ignorant people. Middle- and upper-class people tend to be more honest than lower-class people.
- ✓ The easier it is to cheat and steal, the more people will do so.
- ✓ Individuals have different needs and therefore different levels at which they will be moved to lie, cheat, or steal
- ✓ Lying, cheating, and stealing increase when people have great pressure to achieve important objectives.

The struggle to survive generates deceit. People lie, cheat, and steal on the job in a variety of personal and organizational situations. The ways that follow are but a few:

1. Personal variables Aptitudes/abilities Attitudes/preferences Personal needs/wants Values/beliefs.

2. Organizational variables Nature/scope of the job (meaningful work) Tools/training provided Reward/recognition system Quality of management and supervision Clarity of role responsibilities Clarity of job-related goals Interpersonal trust Motivational and ethical climate (ethics and values of superiors and coworkers)

3. External variables Degree of competition in the industry General economic conditions Societal values (ethics of competitors and of social and political role models)

Question No 6. WHO IS VICTIMIZED BY FRAUD MOST OFTEN?

One might think that the most trusting people are also the most gullible and therefore most often the victims of fraud. Using that rationale, we could postulate that organizations with the highest levels of control would be least susceptible to fraud. But organizations that go overboard on controls do not necessarily experience less fraud; and they have the added burden of higher costs. Controls to protect against fraud by either organization insiders or outside vendors, suppliers, and contractors must be adequate; that is, they must accomplish the goal of control—cost-feasible protection of assets against loss, damage, or destruction.

Cost-feasible protection means minimal expenditures for maximum protection. Creating an organizational police state would be control overkill. A balanced perspective on controls and security measures is the ideal, and that may require involving employees in creating control policies, plans, and procedures. A balanced perspective weighs the costs and benefits of proposed new controls and security measures. It means that a measure of trust must exist among employees at all levels. Trust breeds loyalty and honesty; distrust can breed disloyalty and perhaps even dishonesty. Fraud is therefore most prevalent in organizations that have no controls, no trust, no ethical standards, no profits, and no future. Likewise, the more these circumstances exist, the higher the risk of fraud.

Question No 7. What is meant by FRAUD TAXONOMIES?

Most technical books have a glossary at the end. This one provides taxonomy at the beginning to lay a simple but expanded foundation for what follows in the text. Another benefit of the taxonomy is that it provides a periodic quick review and thus reinforces the lessons learned at the first reading. In essence, the taxonomy summarizes the major principles of fraud auditing and forensic accounting.

Fraud, in a nutshell, is intentional deception, commonly described as lying, cheating, and stealing. Fraud can be perpetrated against customers, creditors, investors, suppliers, bankers, insurers, or government authorities (e.g., tax fraud), stock fraud, and short weights and counts. For our purposes, we will limit coverage to frauds in financial statements and commercial transactions. Consumer fraud has a literature of its own. Our aim is, there-fore, to assist accountants and investigators in their efforts to detect and document fraud in books of account.

Criminal and Civil Fraud

A specific act of fraud may be a criminal offense, a civil wrong, or grounds for the rescission of a contract.

Criminal fraud requires proof of an intentional deception.

Civil fraud requires that the victim suffer damages. Frauds in the inducement of a contractmay vitiate consent and render a contract voidable.

Criminal fraud denotes a false representation of a material fact made by one party to another party with the intent to deceive and induce the other party to justifiably rely on the fact to his/her detriment (i.e., his injury or loss).

Fraud for and against the Company

Fraud can be viewed from yet another perspective. When we think of fraud in a corporate or management context, we can perhaps develop a more meaningful and relevant taxonomy as a framework for fraud auditing. Corporate frauds can be classified into two broad categories:

(1) Frauds directed against the company, and

(2) Frauds that benefit the company.

In the former, the company is the victim; in the latter, the company, through the fraudulent actions of its officers, is the intended beneficiary. In that context, we can distinguish between organizational frauds that are intended to benefit the organizational entity and those that are intended to harm the entity. For example, price fixing, corporate tax evasion, violations of environmental laws, false advertising, and short counts and weights are generally intended to aid the organization's financial performance. Manipulating accounting records to overstate profits is another illustration of a fraud intended to benefit the company but that may benefit management through bonuses based on profitability or stock prices in the market. In frauds for the organization, man-agreement may be involved in a conspiracy to deceive. Only one person may be involved in a fraud against the organization, such as an accounts payable clerk who fabricates invoices from a nonexistent vendor, has checks issued to that vendor, and converts the checks to his own use. Frauds for the company are committed mainly by senior man-agers who wish to enhance the financial position or condition of the company by such ploys as overstating income, sales, or assets or by understating expenses and liabilities. In essence, an intentional mis-statement of a financial fact is made, and that can constitute a civil or criminal fraud. But income, for example, may also be intentionally understated to evade taxes, and expenses can be overstated for a similar reason. Frauds for the company by top managers are usually to deceive shareholders, creditors, and regulatory authorities. Similar frauds by lower-level profit-center managers may be to deceive their superiors in the organization, to make them believe the unit is more profitable or productive than it is, and thereby perhaps to earn a higher bonus award or a promotion. In the latter event, despite the fact that the subordinate's overstatement of income, sales, or productivity ostensibly helps the company look better, it is really a fraud against the company.

Frauds against the company are intended to benefit only the perpetrator, as in the case of theft of corporate assets or embezzlement. The latter specific category of fraud is often referred to as misappropriations of assets. Frauds against the company may also include vendors, suppliers, contractors, and competitors bribing employees. Cases of employee bribery are difficult to discern or discover by audit, because the corporation's accounting records generally are not

manipulated, altered, or destroyed. Bribe payments are made under the table or, as lawyers say, "sub rosa." The first hint of bribery may come from an irate vendor whose product is consistently rejected despite its quality, price, and performance. Bribery may also become apparent if the employee begins to live beyond her means, far in excess of salary and family resources. Several other financial crimes do not fit conveniently into our schema here but also are noteworthy: for example, arson for profit, planned bankruptcy, and fraudulent insurance claims.

Internal and External Fraud

Frauds referred to as corporate or management frauds can be categorized as internal fraud to distinguish them from external fraud (a category that includes frauds committed by vendors, suppliers, and contractors who might overbill, double bill, or substitute inferior goods). Customers may also play that game by feigning damage or destruction of goods in order to gain credits and allowances. Corruption in the corporate sense may be practiced by outsiders against insiders, such as purchasing agents, for example. Corruption can also be committed by insiders against buyers from customer firms. Commercial bribery often is accompanied by manipulation of accounting records to cover up its payment and protect the recipients from the tax burden.

Management and Nonmanagement Fraud

Corporate or organizational fraud is not restricted to high-level executives. Organizational fraud touches senior, middle, and first-line management as well as non-management employees. There may be some notable distinctions between the means used and the motivations and opportunities the work environment provides, but fraud is found at all levels of an organization—if one bothers to look for it. Even if internal controls are adequate by professional standards, we should not forget that top managers can override controls with impunity, and often do so. In addition, even the best of internal controls suffers from atrophy, to the degree they depend on human intervention. This effect is measured by "effectiveness" of internal controls, to ensure they are functioning at the level designed and intended, and not at some subordinate level due to slackness on the part of employees responsible for elements of the control.

Question No 8. Evolution of a typical fraud?

Most frauds follow a similar pattern in the life cycle of the processesor steps. There are differences to consider depending on the fraud. For example, a skimming fraud scheme is "off the books" and therefore requires no real concealment of the fraud. Likewise, the motivation for financial statement frauds is usually very different from that of asset misappropriation frauds.

A general evolution of a typical fraud follows.

1. Motivation/Pressure

- Need
- Greed
- Revenge

2. Opportunity

- Access to assets, records, and/or (control weaknesses) documents that control assets
- No audit trails or separation of duties
- No rotation of duties
- No internal audit function
- No control policies
- No code of ethics

3. Rationalization

Rationalization of the crime as (formulation of intent) borrowing, etc., not stealing

4. Commit the Fraud

- Execute the particular fraud scheme;
- Fraud, theft, embezzlement, etc

5. Convert to Cash

If it is not a cash theft, the fraudster must convert the theft to cash (e.g., theft inventory, financial fraud to stock to cash, or cashing a check made out to a bogus or real payee

6. Conceal the Fraud

- Alter documents and/or records Forgery Destruction of records
- (For skimming and other off-the-books frauds, no concealment is necessary.)

7. Red Flags

- Variances detected
- Allegations made
- Behavior pattern change noted in the fraudster
- (If it is an on-the-books scheme, red flags are likely to occur in the accounting records and data. But even off-the-books schemes exhibit the behavioral red flags.)

8. Audit Initiated

Detection of fraud or discrepancies detected by some method (tips most common; also internal controls, accident, and internal audit are common methods)Anomalies identified and deter-mined to be fraudulent in nature.

9. Investigation Initiated

Evidence gathered Loss of assets confirmed and documented Interrogation of third parties, employees with knowledge, and suspect conducted

10. Disposition

- Employee terminated for cause
- Fraudster Terminated(often management does not desire to pursue legal disposition for various reasons)
- Insurance claim filed

- Criminal prosecution sought
- Prosecution Recommended
- Civil recovery sought Insurance claim filed

11. Trial

Presentation of facts and testimony some of these items are covered in this chapter, at least by way of introduction to basic concepts. The remainder of the book focuses on this list, usually in the sequence listed.

Question No 9. Give BRIEF HISTORY OF FRAUD AND THE ANTIFRAUDPROFESSION.

1. Fraud auditing literature discloses a common theme: Fraud is endemic and pervasive in certain industries, locales, companies, and occupations at particular points in history. For example, railroad promoters in the 1870s raised more capital from less informed investors than ever before. Their fraud, rather simply, was based on more "water" in their stocks. According to some, forensic accounting is one of the oldest professions and dates back to the Egyptians. The "eyes and ears" of the king was a person who basically served as a forensic accountant for Pharaoh, watchful over inventories of grain, gold, and other assets. The person had to be trustworthy, responsible, and able to handle apposition of influence. In the United States, fraud began at least as early as the Pilgrims and early settlers. Since early America was largely agricultural, many frauds centered on land schemes. Perhaps the most infamous colonial era land scheme was the purchase of Manhattan Island, bought from the Canarsie Indians from what is now Brooklyn. The land was bought for trinkets worth about $24. In this case, the Indians tricked the white man, as the Canarsie Indians sold land not even connected to Manhattan Island. Land swindles grew as America expanded west and continue to this day to be a major target of fraudsters and con artists. So much so that the phrase "If you believe that, I have some swampland in Florida I would like to sell you!" has become a colloquialism. The advent of business organizations created new opportunities for fraud. The earliest corporations were formed in seventeenth-century Europe. Nations chartered new corporations and gave thempublic

missions in exchange for a legal right to exists, separation of ownership from management, and limited liability that protected shareholders from losses of the business entity. One such corporation, the Massachusetts Bay Company, was chartered by Charles I in1628 and had a mission of colonizing the New World. The first major corporate fraud is probably the fraud known as the South Sea Bubble.

2. The South Sea Company was formed in 1711with exclusive trading rights to Spanish South America. The company made its first trading voyage in 1717 and made little actual profit to offset the £10 million of government bonds it had assumed. South Sea then had to borrow £2 million more. Tension between England and Spain led to the capture of South Sea ships by Spain in1718. In 1719, the company proposed a scheme by which it would take on the entire remaining national debt in Britain, over £30 mil-lion, using its own stock at 5% in exchange for government bonds lasting until 1727. Although the Bank of England offered also to assume the debt, Parliament approved the assumption of the debt by the South Sea Company. Its stock rose from £128 in January 1720 to£550 by the end of May that year, in a speculation frenzy

The company drove the price of the stock up through artificial means; largely taking the form of new subscriptions combined with the circulation of pro-trade-with-Spain stories designed to give the impression that the stock could only go higher. Not only did capital stay in England, but many Dutch investors bought South Sea stock, thus increasing the inflationary pressure.

3. Other joint-stock companies then joined the market, usually making fraudulent claims about foreign ventures, and were nicknamed "bubbles." In June 1720, the Bubble Act was passed, which required all joint-stock companies to have a royal charter. Partly because it hada royal charter, the South Sea Company shares rocketed to £890 in early June 1720. The price finally reached £1,000 in early August; and a sell-off that began in June began to accelerate. The sell-off was begun largely by directors themselves cashing in on huge stock profits. As the stock price began to decline, the company directors attempted total up and prop up the stock (e.g., having agents buy stock) but to no avail—the stockholders had lost confidence and a run started in September. By the end of the month, the stock price dropped to a low of £150.With investors outraged, and as many of them were aristocrats, Parliament was recalled in December and an

investigation began. As part of that investigation, an external auditor, Charles Snell, was hired to examine the books of the South Sea Company.

This hiring was the first time in the history of accounting that an outside auditor was brought in to audit books, and marks the beginning of Chartered Accountants in England and thus the beginning of Certified Public Accountants (CPAs) and financial audits as we know them today. Thus CPAs owe their profession, at least to a large extent, to a fraud. Cases in more recent history have birthed forensic accountants and fraud auditors: namely, a scandal, the threat of a lawsuit or bankruptcy, and the need to have an expert dig deep into the accounting records. These historical facts are significant among the other frauds of times past, and are why this case is presented. In 1721, Snell submitted his report. He uncovered widespread corruption and fraud among the directors in particular and among company officials and their friends at Westminster. Unfortunately, some of the key players had already fled the country with the incriminating records in their possession. Those who remained were examined and some estates were confiscated. At about the same time, France was experiencing an almost identical fraud from a corporation known as the Mississippi Company that had exclusive trading rights to North America in the French-owned Mississippi River area. Using similar tactics of exaggerating the potential profits, the company owner, John Law, was able to cause a frenzied upward spiral of its stock prices, only to see it collapse after the Regent of Orleans dismissed him in 1720. The company sought bankruptcy protection in 1721. Like South Sea, it was a fraud perpetrated by the exaggerations of executive management.

In 1817, the Meyer v. Sefton case involved a bankrupt estate. Since the nature of the evidence was such it could not be examined in court, the judge allowed the expert witness who had examined the bankrupt's accounts to testify to his examination. Forensic pioneer Dr. Larry Crumbly considers this accountant to be the first forensic

A major savings and loan scandal hit hard in the early 1980s, preceding the energy and telecommunication companies' frauds in the 1990s. The latter led the seeming explosion of fraud around the last half of the 1990s and the early 2000s. During this period, high-dollar frauds reached all types of industries. For example, Waste Management in trash services, Enron in

energy, WorldCom in telecommunications, Adelphia in media, Fannie Mae in government, and HealthSouth in health services all occurred during this time.

Several of these frauds were among the largest ever, and they occurred during a short period of time. Although the cost of the WorldCom fraud was far greater, the most notable fraud, as far as impact on the business community, is probably Enron. In 2001, Enron filed bankruptcy after disclosing major discrepancies in revenues and liabilities in its financial reports. The audit firm Arthur Andersen came to an end as a result of the ramifications of the Enron scandal by 2002. In 2002, the U.S. Congress passed the Sarbanes-Oxley Act (SOX) due to that fraud and others, such as WorldCom. Perhaps nothing has brought more attention to fraud audits and forensic accounting than the Enron scandal and SOX. Are all of these events merely historical flukes? Did media attention create them? Perhaps. Media attention may have created the original public awareness, but the frauds and corruption were there all the time, and there exists no real way of measuring or comparing them. Part of the problem during the period of time when such large frauds occurred was the mind-set of the auditors, which has since turned around completely. Nothing is taken for granted anymore, and the financial well-being of the general public is again the ultimate concern. Suspicion fell on industries, professions, and various areas of government. The undivided attention of auditors, regulators, management, and employees then led to wholesale charges of fraud, theft, and corruption. The fraud environment can be and is often viewed as a pendulum, swinging from one extreme to the other with little time in between at the proper balancing point. After 2002, the pendulum was close to an extreme end, one that entailed ultra-conservatism on the part of companies, and auditors as well, and the stiffest requirements and enforcement by regulators and legislators. This cycle (pendulum swing) is a natural result of human nature, business cycles, and the nature of legislation and regulation. The cycle can certainly be influenced and con-trolled to some extent, but it will never cease.

Question No 10. Auditors Mind set

The argument for mind-set does not quite hold for many of the financial frauds around the turn of the millennium. Of those, most were caught by whistleblowers or the financial collapse of the entity. In some cases, too many people, including auditors, regulators, and company employees, knew, and someone eventually had the ethics and the courage to report the fraud. After the initial attention to these large frauds, those same entities (auditors, regulators, company management, etc.) felt pressure to uncover any frauds and did, continuing the fraud wave.

Fraud auditing, forensic accounting, and/or fraud investigation (i.e., forensic accounting) put things together rather than taking them apart, as is the case in classic financial auditing or the modern method of systems analysis. The process of forensic accounting is also some-times more intuitive than deductive, although both intuition and deduction play important parts. Financial auditing is more procedural in many regards and is not intended to work as effectively in detecting frauds as the tenets of fraud auditing and forensic accounting. Mind-set, not methodology, is probably going to be the best detection of frauds from Enron forward—not a mind-set of paranoia, which trusts no one and sees evil everywhere, but a mind-set trained or experienced to identify the signs of fraud, the most effective means of detecting frauds, and the natural tendency to question the substance of the matter. The term professional skepticism is often used in this regard and applies to financial, fraud, and forensic accounting. In addition to skepticism, fraud auditors should recognize that:

Fraud can be detected as well as discovered by accident or tip.

- ✓ Financial audit methodologies and techniques are not really designed to detect fraud but rather designed to detect material financial misstatements.
- ✓ Fraud detection is more of an art than a science. It requires innovative and creative thinking as well as the rigors of science.
- ✓ Determination, persistence, and self-confidence are more important attributes for a fraud auditor than intelligence. Logic and problem solving and detective skills are critical success factors for fraud auditors and forensic accountants.

Question No 11. Steps in Fraud Investigation.

STEPS IN FRAUD INVESTIGATION

Perhaps a brief overview of a fraud investigation is the best way to con-vey the principles of forensic accounting. In terms of organizational fraud, the objective is to determine whether a fraud has occurred or is occurring and to determine who the fraudster is. In litigation support, the objective is determined by the client. It is important to note that the last step in the process of the investigation is to approach the suspect. That can happen intentionally and accidentally. The intentional approach should be easy enough to avoid, but the accidental requires some extra effort. When an auditor comes across an anomaly (document, accounting transaction, or other evidence of something that "should not be" or a red flag associated with known frauds, or a violation of internal controls), before approaching someone for an explanation, first he should ascertain the probability that the reason for the anomaly is not fraud . The reason for this caution is often when an auditor unwittingly has evidence of a fraud in hand; she goes to a party responsible for the fraud and asks for an explanation for the anomaly. At this point, the investigation at best has been severely hampered and at worst has been compromised for obtaining a confession or conviction in court. For example, an internal auditor notices on performance reports that actual expenses are exactly twice the budget. That is classified, in our terminology, as an anomaly ("should not be"). The natural inclination is to go to the person responsible for authorizing check sin that business unit and ask for an explanation. However, if that per-son is using an authorized maker fraud scheme combined with forged endorsement, he could be cutting two checks for a single invoice—one for the vendor, and one for the fraudster to forge an endorsement and convert to cash. If the auditor does approach that person, either he will come up with a viable excuse, or the auditor could unknowingly offer one. In a real case, the fraudster remained silent, and the auditor said, "You must have paid the vendor twice," to which she replied, "Yes. That is what I did." The fraudster then had the opportunity to replace the stolen funds without getting caught.

Had the auditor assumed it could be fraud, then he would have had the opportunity to gather evidence to determine whether it was error or fraud, and possibly would have found the fraud. But by going to the fraudster, he gave her undetectable exit strategy to the fraud. In other cases,

fraudsters confronted by accident have suddenly retired, burned the business building (to destroy accounting records), or done other things that frustrated any appropriate conclusion to the fraud.

Steps in Investigating a Fraud

The first step is the initialization of the investigation. If it is an organizational fraud, most often that is a tip or an accidental discovery of a fraud.

Predication is necessary to initiate the fraud investigation. Predication is the set of circumstances that would lead the prudent, reasonable, and professionally trained individual to believe that a fraud has occurred, is occurring, or will occur. In litigation support, however, predication is a call from a lawyer. If the specific fraud is not known, or if there is limited information on the fraud, then the next step would be the fraud theory approach. In this approach, the forensic accountant, probably in brainstorming setting, would propose the most likely fraud scheme(if not previously known), and the manner in which that fraud scheme could have been perpetrated on the victim organization. This latter subset is often necessary even in litigation support. Obviously, the forensic accountant needs to be familiar with fraud schemes and red flags associated with each. The theory then serves as the basis for developing a fraud investigation plan. Using the theory, the forensic accountant develops a plan together sufficient and competent evidence (i.e., forensic evidence).This step is where the fraud auditor is particularly applicable. In this step, an examination is made of accounting records, transactions, documents, and data (if applicable) to obtain sufficient evidence to prove or disprove that the fraud identified earlier has occurred. Issues of importance include custody of evidence and other legal matters. After gathering accounting evidence, the forensic accountant will attempt to gather evidence from eyewitnesses, using interviews. This process goes from people the greatest distance from the fraud (not involved but possible knowledgeable), to an ever-narrowing circle of people close to the fraud (firsthand knowledge), to the last step of interviewing the suspect.

Finally, the forensic accountant writes up the findings in a report to the party who him. If the case goes to court, this report, or a similar one, may be necessary during the trial. But regardless, if the case goes to trial, the forensic accountant's work will have to be presented in an effective manner to the judge or jury.

Question No 12. Discuss the Auditor's Liability in reference to Fraud.

Financial auditors who audit public companies are the most common group of auditors and the group most often discussed in terms of auditor liability. While internal, fraud, and outsourced/consulting auditors face similar issues and share the same liability in some cases, differences do exist. The requirements for audits of public companies are mandated at a higher level by federal laws and legally enforceable regulatory standards. In this chapter, financial auditors conducting audits of public companies (also known as external or independent auditors or public accountants), or organizations otherwise subject to the regulations discussed, are the principal focus of discussion. Auditor liability has never been a crystal-clear issue to the public, regulators, or even auditors themselves. Some of the more notable reasons are the amount of judgment and expertise involved in accounting and auditing, public misconceptions, political influence, constantly changing requirements, the substantive and sampling nature of audits, and other environmental factors. Lawmakers and regulators have tried to establish liability definitively in practical terms, but the task isn't an easy one. Financial auditors (internal and external) may still been doubt as to the extent of their legal and professional responsibility for fraud detection when conducting financial audits. Numerous laws and regulatory standards have been put in place in a relatively short period of time and are still maturing. Auditors implementing these requirements will adjust, learn, and become more proficient over time, but now they are still learning both how recent regulations work in practice and the boundaries of their liability.

The general public, as opposed to financial auditors, does not seem to have any doubts about auditor liability, nor do the courts. There is a growing public perception that auditors, by the nature of their education, intuition, and work experience, can and should be able to sniff out fraud wherever and whenever it exists in financial records and/or data. That standard is far higher than anyone in the audit professions has ever advocated or thought reasonably possible. No auditor could ever live up to such a strict standard of care. Nor could any auditor afford the premiums for professional liability insurance if the public's perception of the standard became a legal reality.

The public's perception of auditor responsibility for fraud detection is highly unrealistic and contributes to what is commonly known as the expectations gap. The expectations gap is the difference between what the public thinks a financial audit is and what financial audits really are. Part of the gap stems from a lack of transparency on the part of auditors and audit regulators, who need to educate the public better about the process and content of financial audits, accounting principles and rules, and financial reporting and disclosures. The public's part of the gap is mostly out of uneducated misconceptions. Few people know that financial statement audits are aimed at providing reasonable assurance as to whether a material misstatement in the financial statement exists or not and whether financial transactions are recorded and financial statements are presented inconformity with generally accepted accounting principles (GAAP) or not. That language is nearly synonymous with the financial audit "opinions" issued for financial statement audits mandated by generally accepted auditing standards (GAAS) as promulgated by the American Institute of Certified Public Accountants (AICPA). In addition, GAAS states that the "The auditor has a responsibility to planed perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud."

The public simply assumes that fraud should be caught in a financial audit. Although that is not a false statement, it is not a true one either. Outside of the aforementioned misconception about the purpose of financial statements, the process and procedures within a financial audit are also misunderstood. Financial auditors, to some extent, rely on management's (or otherwise the entity's) representations; it is impractical and would be unreasonable for auditors to try to absolutely, perfectly, unquestionably determine whether financial statements were accurate and in compliance with regulations. Also, financial audits occur mostly after the end of the period being audited (although notably the trend is for more audit work to be done within the period). As with other crimes, the more time that goes by after a fraud has been committed, the harder it is to catch. Audit procedures traditionally have not directly targeted fraud, although that is changing. The changes mainly stem from two new regulations.

Increased Auditor Liability

Growing concern and expectation of the public and Congress culminated in the advent of the Sarbanes-Oxley Act of 2002 (SOX) and the adoption of Statement on Auditing Standard (SAS) No. 99,

Consideration of Fraud in a Financial Statement Audit

Since those documents were put in place, even more attention has been brought on the issue of auditors detecting fraud, and of course more technical guidance has been provided for financial auditors. SOX address the financial auditor's responsibility to detect fraud in direct and indirect tenets. Indirectly, for example, the Public Companies Accounting Oversight Board (PCAOB) was created in reaction to public and congressional perception that large financial frauds had happened while being audited by large financial audit firms that were not performing their professional duties appropriately and that were not being properly regulated by the AICPA. These aspects of SOX and PCAOB lead us to believe that the PCAOB's creation was a simultaneous reaction with SOX:

- ✓ The PCAOB answers directly to the Securities and Exchange Commission (SEC). Prior to the passage of SOX, the Financial Accounting Standards Board (FASB) and the American Institute of Certified Public Accountants (AICPA) were delegated authority under the SEC, but did not report directly to the SEC.
- ✓ An examination of the quality of audits of SEC firms now is per-formed periodically not only by peers (other public accounting firms in a peer review) but also by the PCAOB.

In order to conduct financial audits of SEC companies, a financial audit firm must be registered with the PCAOB. The members of the PCAOB are not all CPAs; two of them can-not be CPAs or former CPAs. All members of the FASB, the practical authority for accounting standards, have been CPAs or former CPAs.All of these aspects point to two main regulatory changes: a tighter link of control between the law and the entities under the law and independent supervision and monitoring.SOX and SAS No. 99 have increased the expectation that auditors will detect fraud; auditor liability has also increased. By definition, auditors are now held liable

for SOX and SAS No. 99 requirements, both of which explicitly or implicitly imply that auditors must consider fraud and must perform specific procedures to detect fraud.

Question No 13. Evidence play vital role in any case. Explain Basic Forms of Evidence.

EVIDENCE

In general, evidence consists of anything that can be used to prove something. .In a legal sense, evidence means an assertion of fact, opinion, belief, or knowledge whether material or not and whether admissible or not.

Evidence rules are principles developed and refined over hundreds of years, that are designed to ensure that only relevant and probative evidence is admitted in court proceedings, and that irrelevant, unreliable and prejudicial evidence is excluded, so that cases can be fairly and expeditiously decided.

Every aspect of trying a case from filing the complaint through discovery, into the presentation of witnesses and exhibits-is affected by rules of evidence. This body of law covers not just what counts as evidence, but how that evidence is gathered, handled, and presented.

The rules of evidence are complex and counsel should be contacted if an important question of evidence arises. Additionally, rules of evidence vary by jurisdiction, even within the same country. For example, in the United States, state courts have different rules for the admissibility of evidence than do federal courts. The following are some general principles regarding evidence; therefore, it is very important to review the rules for your area.

Three Basic Forms of Evidence

Evidence is anything perceptible by the five senses, which is invoked in the process of arguing a case. Documents, spoken recollections, data of various sorts, and physical objects are all potentially evidence. Evidence is simply anything that relates to the proving or disproving of a fact or consequence. With the known universe available for court inspection, legal authorities have narrowed the field by setting up categories to evaluate evidentiary significance.

There are three basic forms, as distinguished from types, of evidence: testimonial, real, and demonstrative. Testimony refers to the oral statements made by witnesses under oath. In general, there are two types of testimonial witnesses: lay witnesses and expert witnesses. A lay (or fact) witness is a non-expert witness who must testify from personal knowledge about a matter at issue. An expert witness is a person who, by reason of education, training, Skill, or experience, is qualified to render an opinion or otherwise testify in areas relevant to resolution of a legal dispute.

Real evidence describes physical objects that played a part in the issues being litigated. The ***term*** includes both documentary evidence-such as cancelled checks, invoices, ledgers, and letters-as well as other types of physical evidence. Therefore, a typewriter or printer in a case involving questioned documents is clearly real evidence, as is a tape recording, since members of the court can experience the sounds firsthand.

Demonstrative evidence is a tangible item that illustrates some material proposition (e.g., a map, a chart, a summary). It differs from real evidence in that demonstrative evidence was not part of the underlying event; it was created specifically for the trial. Its purpose is to provide a visual aid for the jury. Nonetheless, it is evidence, and can be considered by the jury in reaching a verdict.

Direct Versus Circumstantial Evidence.

There are two basic types of admissible evidence: direct evidence and circumstantial evidence. *Direct evidence* includes testimony that tends to prove or disprove a fact in issue directly, such as eyewitness testimony or a confession. *Circumstantial evidence* is evidence that tends to prove or disprove facts in issue indirectly, by inference. Many fraud cases are proved entirely by circumstantial evidence, or by a combination of circumstantial and direct evidence, but seldom by direct evidence alone. The most difficult element to prove in many fraud cases-is usually proved circumstantially, and necessarily so, because direct proof of the defendant's state of mind, absent a confession or the testimony of a co-conspirator, is impossible.

In a circumstantial case, the court may instruct the jury that. The prosecution must exclude all inferences from the facts other than its determination of guilt. Even if no such instruction is

given, the Certified Fraud Examiner should apply the same standard in preparing a circumstantial case.

Relevance

The admissibility of evidence depends on a wide variety of factors-and, in large part, on the discretion of the trial judge-but the most important factor is relevance. Relevant evidence is evidence that tends to prove or disprove a fact in issue. The facts in issue, of course, vary according to the case, but generally can be said to be those that tend to prove the essential elements of the offence or claim as well as related matters such as motive, opportunity, identity of the parties, and credibility.

Whether a particular piece of evidence is relevant or not depends on what the evidence is offered to prove. An item of evidence might be relevant and admissible if offered to prove one thing, but not relevant and inadmissible if offered to prove something else. For example, evidence of other crimes, wrongs, or acts committed by the defendant would be admissible if offered to prove that the defendant is generally a bad person, and therefore is likely to have committed the crime with which he is charged. However, evidence would be admissible if offered to prove motive, intent, identity, absence of mistake, or modus operandi, if such factors are at issue. If evidence of other wrongs or acts is admitted, the judge will instruct the jury that they may consider the evidence only as it relates to the narrow issue for which it was admitted, and may not consider it for any other purpose.

That evidence is relevant does not, however, automatically mean that it will be admitted. Relevant evidence still might be excluded if it is unduly prejudicial, threatens to confuse or mislead the jury, or to cause unnecessary delay, waste of time, or is merely cumulative. Relevant evidence also might be excluded if it is subject to certain privileges. Thus, evidence of drug addiction technically might be relevant to prove motive for embezzlement or fraud, but the judge still might exclude the evidence if he believes that its probative value is outweighed by the danger of prejudice to the defendant

Question No 14. Discuss Special Problems Concerning Some Types of Circumstantial Evidence.

Special rules govern certain types of evidence, which have been found over the years to be so misleading and prejudicial that they have been categorically excluded. Such evidence is always excluded unless an exception applies.

Character Evidence

In civil and criminal trials, there is strong policy against character evidence. Character evidence (sometimes called propensity evidence) is testimony or exhibits that purport to establish a "trait of character" or propensity to behave in a particular way, such as care flutiness, honesty, violence, or cowardice. There are some good reasons to leave character out of the discussion whenever possible.

First, the subjective nature of the description-one person's "grufP'is another viewer's "aggressive."

Additionally, character is not an absolute indicator of behaviour. That is, it is pretty common to remark how "out of character" somebody's actions were in a given situation. So there is always a chance someone was acting out of character, making the behavioural propensity (if there was one) useless in the legal exchange.

Finally, testimony about character has a reckless potential to be mistakenly founded, misled. It is always possible to "misjudge" someone, especially if we only know the person in limited circumstances like work or a social club. Moreover, it is exceedingly easy to fabricate incidents about character and, for shrewd talkers, to manipulate perceptions of personality. In a fraud case, it must be shown that the defendant committed the act in question. There is too great a danger of prejudicing the jury if you allow testimony about the defendant just being a bad person. Whether he is a bad person or not ought to have no bearing on whether or not he committed the act in question.

Exception to the Character Rule

In civil cases, character evidence is rarely admissible. In criminal cases, there are some instances where character evidence is relevant to the charge at hand. For example, if the mental condition or legal competency of the accused is in question, character evidence is allowable.

In addition, the courts recognize certain exceptions to the general rule that character evidence is inadmissible in criminal cases. Some of the exceptions for use of character evidence in criminal cases include:

The accused may offer evidence of his or her good character, in which case the prosecution may introduce evidence of the accuser's pad character .Character evidence may be admissible to reflect on the credibility of a witness Although evidence of other crimes, wrongs, or acts is generally not admissible to prove the character of a person; there are some uses of character evidence that may be admissible because they are offered for a purpose other than showing character. Some of the exceptions for use of character evidence in criminal cases may include .

- ✓ To show the accuser's knowledge, intent, or motive for the crime
- ✓ To prove the existence of a larger plan of which the charged crime is apart.
- ✓ *To* show the accuser's preparation to commit the charged crime
- ✓ To show the accuser's ability and means of committing the crime (possession of a weapon, tool, or skill used in the commission of the act)
- ✓ To show that the accuser's opportunity to commit the crime .Threats or expressions of ill Will by the accused

Question No 15. What you mean by Opinion Testimony. Also explain the Exceptions to the opinion Rule.

Opinion Testimony

Generally, lay (i.e., non-expert) witnesses are only allowed to testify about what they have actually experienced firsthand, and their factual observations. Witnesses provide a report on what they know, and keep their opinions and conclusions to themselves.

Exceptions to the Opinion Rule

NON; EXPERT WITNESSES

Despite the general rule, there are ways to get a non-expert witness's opinion into the record. For example, an employee at a securities f1rtn blows the whistle on his superiors for a high- level stock fraud. Defense suggests the investigation was an invasion of privacy, Prosecutors are justifying their secret eight month investigation on the basis of the whistleblower's tip, the prosecution will enter the whistler's "opinion" and his suspicions of fraud to show that the government was justified in conducting its investigation. In this case, the opinion is admissible; however, the reason it is allowed in is not to show that management is guilty, but to show what prompted the investigation.

Opinions are admissible if they pass a three-part test:

Does the witness have direct personal knowledge of the facts to which the opinion pertains?

Is the opinion of the common, everyday sort, i.e." does not involve specialized knowledge or tests?

Is the opinion NOT part of a level judgment, reserved for the jury or judge to decide?

Opinions from ordinary witnesses must be based on personal experience and have some bearing on the *facts* (as opposed to the *judgment* of the case. This distinction is further refined in situations involving hearsay and personal judgment, discussed below. Expert witnesses are exempt from the opinion rule, since experts are hired to render a professional opinion.

EXPERT WITNESSES

Expert witnesses are allowed to give opinion testimony because they possess education, training, skill, or experience in drawing conclusions from certain types of data or information that lay

witnesses do not possess. However, expert testimony may be excluded if it embraces a legal conclusion. Therefore, expert opinions addressing or innocence will likely be excluded in criminal cases.

Exhibits

Exhibits are the tangible objects presented as evidence. Therefore, both real evidence and demonstrative evidence are entered into the record as exhibits. This includes documents like contracts, letters, and receipts; plus photographs, X-rays, baseball bats, knives, fountain pens. In short, anything that is not testimony is an exhibit Testimony is what people say. Exhibits are the "props."

Demonstrative Exhibits

An exhibit used for purely "illustrative purposes" is a type of *demonstrative evidence.* Demonstrative evidence includes charts, and summaries that help to simplify complicated evidence for the jury. Such evidence is admissible if the court decides that it presents a fair and balanced summary or picture of the evidence and is not unduly prejudicial.

In complex fraud cases, such evidence is extremely useful, but care should be taken to keep the charts and exhibits simple. The evidence that is summarized must be made available to the other party, and the court may order that the underling document may be produced to the court.

Authenticating Typical Exhibits

At the most basic; level, evidence must be established as reliable or authentic. Thus, evidence, other than testimonial evidence, must be properly authenticated; that is, the party offering the document must produce some evidence to show it is, in fact, what the party says it is. If a piece of real evidence cannot be authenticated, the evidence Will not be admitted, even if it is plainly relevant.

Similar to the authentication requirement for evidence, there is a sinlilarsort of "credibility test' for witnesses. If testimony is to become admissible evidence, the witness must demonstrate that the knowledge being communicated is believable and made by personal experience.

Question No 16. There are some of the issues you Will encounter in proving to the Judge that a particular exhibit is authentic.

Diagrams

A diagram (on paper or some other tangible display) can be admitted as evidence with no more foundation than the witness: "Is this a fair representation of the Suite where you work?" It does not have to be true to scale, or particularly detailed. A diagram can be prepared before trial, during trial, or prepped outside the court and finished during questioning. If the witness or the opposition objects to the diagram, further foundation may need to be established. Diagrams can be used in random with photos *or* other representational evidence, or as assistance in demonstrations to the jury.

Correspondence

Letters and faxes require a foundation to establish authorship. Depending on the document and situation, the foundation is laid in one of several ways: (1) the author is present and claims authorship; (2) a witness testifies to seeing the author write the document; (3) with handwritten letters, a witness verifies the author's penmanship; (4) with typed or machine- written documents, the witness verifies the author's signature; (5) a witness testifies that the contents of the document point decisively to the author. These and many other document issues may require the participation of a *questioned documents expert*. These professionals are trained to analyze virtually every aspect of document production, from handwriting to the approximate strength of the letter "a" when struck from a particular manual typewriter.

Business Records

Business records can encompass a broad range of documents, from all sorts of Organizations, including corporations, small businesses, nonprofit operations, and community groups.

Exhibits such as business records and correspondence are vulnerable to objections as hearsay.

To overcome a hearsay objection with regard to business records, you must show the following:

The document was prepared as a usual part of doing business (i.e., it was not prepared specifically for litigation).

The document was prepared reasonably near the time of the event it describes. .The organization's way of keeping records is demonstrably reliable.

This can be accomplished by having a member of the record-keeping or archival staff testify how records are kept and that these particular records were created in the normal course of business. .

The requirements for government documents are the same as for other business records: The distinction between government and business records arose because of narrow

Interpretations of the law that separated nonprofit from for-profit enterprises. Today, most records, regardless of origin, are called business records.

Digital Evidence

Courts are still sorting out the issue of how to deal with digital evidence, and there is still much controversy regarding how to authenticate digital records. If digital evidence needs to be seized, it is vital that you engage the services of a trained computer forensic technician. A properly trained technician should know the proper procedures to follow to ensure the files can be authenticated.

In the case of computerized business records, many courts will allow such records into evidence as long as they meet the usual business-records foundation. The required supporting material to authenticate computer records will include information on the computing machine used, any software, and the record-keeping process. A business record, electronic or otherwise, is legal as long as it is kept in the normal course of business. When there are clear routines for compiling information, admitting the record into court will be routine.

Photographs

Photographs can be tricky: they need foundation to establish their fidelity to the 6bject they claim to represent. Generally it is enough to have a witness familiar with the object or space in a photo to corroborate, "Yes, that's the hallway running between our two buildings." The matter

gets more complicated when a photo is controversial. This can require technical specifications for proper foundation.

ln some unusual situations, a photo may reveal information, which no 'witness can corroborate. There has been at least one instance where the background of a photo showed a stabbing that took place in a crowd. No one, not even the photographer, saw the stabbing at the time. In unusual situations where a photo communicates evidence not substantiated elsewhere, the foundation of the photograph will need more strength-including technical details on the camera, the f11m, who took the shot, why and where, etc.

The exceptions make photos seem more legally fraught than they are. They usually ate admitted with little objection. Photos do not even have to be contemporary with the crime or grievance to which they pertain. If a photograph is established as accurate in its portrayal, it can be shot after the original act.

General Points

Either side can enter exhibits into the record, given the proper foundation. Once admitted, the evidence is available for use by either side. It does not matter who entered a hammer into evidence; either side can use it during questioning.

It also does not matter when exhibits are admitted. They may be introduced into evidence during direct examination: opposing counsel is allowed to inspect the exhibit; the witness confirms the exhibit, which has been marked Exhibit A (or Exhibit l): Some courts use letters for exhibits while some court use numbers. Usually the exhibit is identified by which side enters it (e.g., Plaintiff's Exhibit 1).

When everyone agrees, exhibits cart be directly entered into the record, without foundational review, by a simple stipulation. Both parties sign the stipulation form, describing and acknowledging the exhibit.

Question No 17.Discuss the best evidence Rule and also explain the objections to exhibits.

The "Best Evidence" Rule

Sometimes testimony may be rejected because of the "best evidence "rule. This prohibits a party from testifying about the contents of a document without producing the document itself. Also known as the "original writing" rule, it requires that when a witness testifies about the contents of a document, at least a fair copy of the original must be available for inspection.

If there is not an original, a copy of the proven authentic document will do. If the document is lost-no original, no copies-the judge will have to be convinced there is good reason to forgo the exhibit and admit the testimony. Fraud examiners can use copies in preparing their case reports, but at trial the original must be produced if it is available. Certified copies of public records should always be obtained.

Objections to Exhibits

Just because an exhibit is authenticated does not mean it is automatically admitted. If the evidence violates some other rule of evidence-such as the rules again.st hearsay, prejudice, or relevance"-'-the exhibit is barred.

Exhibits sometimes require separate hearings for the judge to consider admitting the material or not. Fraud trials can be bogged down with lengthy challenges to the sometimes mountainous stacks of documents offered as evidence. In deciding on the admissibility of exhibits, judges can decide to admit the material just as it is, admit it with alterations (such as expurgating parts of a text or obscuring certain images), or deny the admission altogether.

Chain of Custody

Chain of custody issues, like those discussed regarding experiments above, are paramount issues in any case, affecting every piece of physical evidence. Chain of custody refers to (1) who has had possession of an object, and (2) what they have done with it. This rule is especially pertinent to the discovery process, since discovery is the appropriate stage to be conducting tests and otherwise inspecting evidence. Gaps in the chain of custody (when it is not clear what occurred

with a set of records, for example) or outright mishandling (a group of questioned documents was not properly sealed; perhaps), can dishevel a case but not wreck it outright.

Courts have found in some cases that even though there have been mistakes in the chain of custody, the mistake affects the "weight" though not the "admissible if' of evidence. That is to say, the evidence will still be allowed into the record, but will be accompanied by a forthright description of any improprieties, which have occurred in the chain. The jury and judge are supposed to consider the improprieties when they deliberate, "Weighing" the case for ~t or innocence. In fraud cases, the array of physical evidence, all the paper documents, audio and video recordings, and information-processing equipment, such as computers, demands some close monitoring in the chain of custody.

The following are some general guidelines that will help you demonstrate the chain of custody. They will also help you in authenticating the evidence you receive:

If records are received via mail or courier-receipted delivery, keep copies of the postmarked envelope or the delivery receipts.

If a cover letter is included, make sure you keep it.

If the cover letter or transmittal letter includes a list of the documents, check the package immediately to ensure all documents are there. If something is missing, make a note in the file and notify ~e sender immediately.

If you receive documents in person, create a memo stating the date and time the documents were received; who gave you the documents, where that individual obtained the documents, and a complete list of the documents received.

If you obtained the documents yourself from the original source (desk, file cabinet, etc.), create a memo describing the date, time, exact location of where the documents were found, and a complete list of the documents obtained.

Keep the originals of these memos or delivery receipts in the case file and keep a copy with the documents (it will be much easier to identify where the documents came from if you have the information with the documents).

Question No 18. Hearsay has many exceptions. Explain the exceptions to the Hearsay Rule.

Hearsay

Hearsay as "a statement, other than one made ...at the trial or hearing, offered in evidence to prove the truth of the matter asserted." Basically, hearsay involves the following elements: .A statement. : This includes anything intended to be an assertion; statements can be oral, Written, or nonverbal conduct, such as nodding ahead.

That is made outside the court's supervision. This includes statements made at trial or during deposition is not hearsay because they are made during court proceedings, but a statement made at work or at a crime scene is outside the court's supervision and could be hearsay if the other elements are also present

That is offered to prove the truth of the matter asserted. A party offers a statement to prove the truth of the 'matter asserted lf the party is trying to prove that the assertion made by the declarant (the person that made the out of court statement) is true.

This sets apart virtually anything said outside the courtroom, or outside an officially designated function of the court like a deposition. Excluding hearsay on one level means witnesses cannot say, "He said she said." Each person testifies to his or her own experience. This is designed to protect the credibility and condition of testimony and to preserve the right to cross-examine witnesses by each side.

Each witness the trial will be questioned about personal, firsthand encounters. Unless their statements satisfy one of the exceptions discussed below , witnesses will speak only about things they have experienced themselves. If possible, evidence should 'be presented in the courtroom so that the jury can determine the weight to give each piece of evidence.

However, the hearsay rule is full of exceptions-ways to get information into the record, even though it is technically hearsay-which accounts for the rule's infamy in courtroom dramas and in real courtrooms. A basic distinction lies with the nature of the statement under consideration. The law is specifically designed to exclude statements which are offered "to prove the truth of

the matter asserted" in the statement.1herefore, any hearsay statement offered to direcdy proves the charge is barred, Simply put, a conviction cannot rest on a "she-said/he-said" (hearsay) recollection.

Exceptions to the Hearsay Rule

The Truth of the Statement Is Not at Issue

The hearsay rule only applies if the statement is being offered to prove the trUth of the matter contained in the statement. Therefore, if the statement is offered for some other purpose, it, technically, is not hearsay. Any out-of-court statement can be admitted if it {1) is relevant to some aspect of the proceedings, and (2) is not offered for the truth of its contents. Most often such statements are used to show a person's knowledge or state of mind at a particular time. For instance, a witness will be allowed to testify that she heard the defendant say, "I can't stand this-company. They owe me big time," The statement cannot be used to prove that the defendant actually stole from the company; however, it can be admitted to show that the defendant's state of mind-that he was disgruntled.

Admissions

Anything spoken or written by a party to a lawsuit can be entered into the record, provided the statement can be corroborated and is relevant. Each side can use its adversary's out-of- court statements as evidence.

For example, during your investigation of the case prior to trial, you interviewed the defendant. During the interview, he tells you that he falsified the invoices. Later he denies making the statement. If you take the stand and tell the jury that the defendant told you he falsified invoices, technically that statement is hearsay. However, since it is an admission, it will be admitted under this exception to the rule.

An admission is not necessarily an outright confession. A witness may testify that a bank officer told her, "I have ways of getting loans approved that no one else knows about." The statement alone does not prove loan fraud against the officer, but it does establish, by his own admission, his stated intent to subvert the security controls of the institution.

In cases involving corporations, large groups, or government agencies, any statement made by a member of the organisation is potentially an admission.. The person who made the statement has to be directly authorized to speak for the organisation, or perform a job related to the issue under discussion.

For example, an agent employed by Jefferson Realtors who says, "You've been defrauded here" to an aggrieved client has made an admission on behalf of the company. A janitor at Jefferson Realtors, however, cannot make the same admission because janitorial duties are not related to the formation of contracts, and chances are the janitor is not authorized to make corporate declarations. On the other hand, an agent makes contracts on the company's behalf, so the statement is an admission even if the agent is not the official spokesperson for Jefferson's legal affairs.

Statement against Interest

A statement against interest is a special form of admission in which a prior statement is at odds with the declarant current claim. In prosecuting a tax evasion charge, for example, prosecutors may present a financial statement used by the defendant to obtain a: loan; this is a statement against interest because the document declares a higher net worth than he now claims to have.

Business and Government Records

We commonly think of invoices, receipts and official documents as the final legal word. Technically speaking, though, business and government records are hearsay; they are prepared outside the courtroom. A special exception for these materials makes them admissible if they are provided with a legal foundation.

The admissibility of records rests on two criteria: whether they were prepared during regularly conducted business activity and whether they are verifiably trustworthy. Materials prepared specifically for trial are not admissible as business records. Anything that casts doubt on the veracity of these documents can bar them. In situations where the charge involves altered documents, the materials are admitted to prove the charge of alteration not for their truth-value- so the hearsay rule does not apply.

Computerized records have had no trouble being accepted as evidence. Generally, the hearsay exception for business records applies (i.e.., as long as the records have been 'compiled as a regular facet of doing business, they are admissible).

Absence of an Entry in Business Records

Evidence that a matter is not included in the memoranda or reports kept in the regular course of business may be admissible to prove that a certain event did not occur, if the matter was one about which a memorandum or report regularly was made and preserved, unless the source of information or the circumstances indicate a lack of trustworthiness.

Recorded Recollections

A memorandum or record about a matter concerning which the wittiness once had knowledge but now has forgotten, and that was made or adopted by the witness when the matter was fresh in memory, and is shown to be accurate, may be admissible. Such memoranda or records also may be shown to a witness who has temporarily forgotten the events in order to refresh the wittiness' recollection and allow the testimony to be more complete or accurate.

Former Testimony

Testimony given by the declarant at another hearing is admissible if the party against whom the testimony is now offered then had an opportunity and similar motive to examine the witness as in the present trial.

Present Sense Impressions

Courts assume that statements made during or immediately after significant events or condition and that describe or explain the event or condition are reliable, so present sense impressions are admissible. For example, a witness can report that he first suspected fraud at Securities Plus by noting that his superior said, "Oh my God! This can't be happening!" when he was informed that there would be an audit. In a similar example, Mr. Whistler notices.]jenny Moore, a co-worker, in John Smith's office and overhears her say, "Oh, here are some bid sheets in the trash can." If the government prosecutes Smith forbid rigging, which is demonstrated by the bid sheets, Mr.

Whistler can testify about Moore's statement as a present sense impression because the words described the scene before her.

Excited Utterances

There is also an exception for statements relating to a startling event or condition made while the declarant was under the stress of its excitement. Unlike statements of present sense in1pressions, excited utterances require an occurrence that is startling enough to produce excitement. In the Mr. Whistler scenario, for example, Moore's statements n:light qualify as an excited utterance if she discovered the bid sheets after months of searching for incriminating evidence and told Whistler, while jumping up and down in excitement, "I've found the evidence I've been waiting for a longtime." Here, the successful conclusion of the search was sufficiently exciting.

Then Existing Mental, Emotional, or Physical Condition

Statements of the declarant then existing state of mind, emotion, or physical condition are also admissible as exceptions to the hearsay rule. Generally, evidence rules list state of mind, emotion, sensation, or physical condition, pain, and bodily health as acceptable subject matter, along with extremely personalized thought processes such as intent, plan, motive, design, mental feeling.

Defense attorneys at a fraud trial sometimes use arguments about what their client intended, or the confusion and stress the person was suffering. For instance, as the defendant was seen shredding documents, he was overheard to say, "They'll never prove anything now." The statement may be admitted to show the defendant's state of mind at the time he was shredding the documents. It also shows that the defendant acted with the intent to destroy the documents. Hearsay statements that help establish this intention are admissible as exceptions.

Statements for Purposes of Medical Diagnosis or Treatment

Anything first communicated during a medical examination is admissible as a hearsay exception. This includes medical history, symptoms, pain, and the general character of the, medical condition. These statements do not even have to have been made by the patient. They can involve someone (parent or spouse) accompanying the patient.

Other Exceptions

Miscellaneous exceptions to the hearsay rule include things like dying declarations and ancient documents. For those instances not specified in any rule, there remains the judge's discretion: anything the judge deems trustworthy for the purposes of its presentation is admissible. This is the cornerstone of the rule. Hearsay is excluded in the first place because it supposedly lacks trustworthiness; however, other kinds of hearsay that do not fall within any specific hearsay exceptions may be admissible it they meet the same standards of trustworthiness as required for the listed exceptions.

Question No 19. Crime investigation is considered tough task Do you agree or not. Also discuss the goals of crime investigation.

Crime Investigation:

A criminal investigation is an official effort to uncover information about a crime. There are generally three ways that a person can be brought to justice for a criminal act. First, and probably the least likely, the individual will be driven by his conscience to immediately confess. Second, an officer of the law can catch him in the act. Third, and most common, a criminal investigation can identify him as suspect, after which he may confess or be convicted by trial.

General Investigation:

In most cases, when a crime is committed, officials have two primary concerns. They want to know who committed the crime, and what the motive was. The reason why a person breaks a law is called the motive.

The motive does not always come after identifying the perpetrator in a criminal investigation. Sometimes the motive is suspected or known and used to catch the criminal. This is often true with crimes such as kidnappings and murders. Notes or other forms of evidence may be left that reveal why the crime has been committed.

Criminal investigations are usually conducted by police. There are other official agencies that have the authority to investigate and launch criminal charges. In the United States, these include the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS).

Police and other officials may use a variety of methods to conduct criminal investigations. Sometimes they work with their canine co-workers. They may also use various scientific techniques such as fingerprint and ballistics analysis.
A controversial investigation method sometimes employed in the US is the use of informants. Many people disagree with this practice because these individuals are generally criminals who are looking to get out of trouble or to reduce their punishments. It is therefore argued that they can be influenced to say or do whatever will please those investigating the case.

There are some parts of a criminal investigation that police may not be able to handle. Some cases require investigation techniques that demand specialized knowledge or training that the investigators or their colleagues may not have. This means that the police may have to employ others to help them. This is especially true with deoxyribonucleic acid (DNA) testing. Although this technique is popular, it is often performed by third-parties.

A criminal investigation does not always yield results. Sometimes suspects are accused only for it to be determined later that they are not guilty. At other times, an extensive criminal investigation may not produce any suspects. This can mean that no one will be punished for the crime that was committed.

Goals of Crime Investigation:

A criminal investigation is the process of discovering, collecting, preparing, identifying, and presenting evidence to determine what happened and who is responsible. Goals of criminal investigations are to:

- ✓ determine whether a crime has been committed
- ✓ legally obtain information and evidence to identify the responsible person
- ✓ arrest the suspect
- ✓ recover stolen property and

- ✓ present the best possible case to the prosecutor
- ✓ Find the guilty party.
- ✓ Exonerate the innocent.
- ✓ If the investigator doesn't preserve the evidence or document that preservation correctly, the evidence isn't useful in court.
- ✓ Crime Laboratory can't make the evidence make sense if it isn't collected correctly.

A successful investigation is one that follows a logical sequence. First, all physical evidence is obtained legally, and all witnesses are effectively interviewed. Then all suspects are legally and effectively interrogated, and all leads are thoroughly developed. Finally, all details of the case are accurately and completely recorded and reported.

Question No 20. Explain the following:

A) Basic Functions of Criminal investigators

B) Effective Criminal investigator

Ans:

Basic Functions of Criminal Investigators

What do criminal investigators do? First and foremost, they provide emergency assistance. They then proceed to secure the crime scene. They photograph, videotape, and sketch the scene; take notes and write reports; search for, obtain, and process physical evidence; obtain information from witnesses and suspects; and identify suspects. Other aspects of their job entail conducting raids, surveillances, stakeouts, and undercover assignments, and testifying in court.

Effective Criminal Investigators

Effective criminal investigators obtain and retain information; apply technical knowledge; and remain open minded, objective, and logical. They are also culturally adroit and skilled in

interacting across gender, ethnic, generational, social, and political group lines. They are emotionally well balanced, detached, inquisitive, suspecting, discerning, self-disciplined, and persevering. Additionally, they are physically fit and have good vision, acute hearing, and a high energy level. It also helps if they have a nosey nature!

Question No 21. Discuss the criminal Investigator Responsibilities and also explain the crime scene priorities.

Criminal Investigators' Responsibilities

Criminal investigators should arrive at the crime scene as quickly as possible because:

- The suspect may still be at or near the scene.
- Injured persons may need emergency care.
- Witnesses may still be at the crime scene.
- A dying person may have a confession or other pertinent information to give.
- Weather conditions may change or destroy evidence.
- Someone may attempt to alter the crime scene.

Crime Scene Priorities

Although circumstances at the crime scene may dictate the criminal investigator's priorities, the first priority generally is to handle emergencies: save life, apprehend suspects, and request assistance. The second priority is to secure the scene. The third priority is to investigate.

Preliminary Investigations: Basic Considerations

The initial response is usually by a patrol officer assigned to the area where a crime has occurred.

During the preliminary investigation, criminal investigators measure, photograph, videotape, and sketch the scene. They then proceed to search for evidence. If the investigators find physical evidence, they identify, collect, examine, and process it. Victims, witnesses, and suspects are questioned, and statements and observations are recorded in notes.

Following are the steps in the investigative process:

- Determine if a crime has been committed.
- Verify jurisdiction.
- Discover all facts and collect physical evidence.
- Recover stolen property.
- Identify the perpetrator or perpetrators.
- Locate and apprehend perpetrators.
- Aid the prosecution by providing evidence of guilt admissible in court.
- Testify effectively as a witness in court.

It is not enough to just collect and analyze evidence. Investigators need to apply the logic of reasoning or the methodology of scientific research investigation. They need what can only be called working theories, which are sufficiently flexible to allow for new information while still demonstrating clear patterns of inference or cause and effect.

A hypothesis is an if-then statement that implies a variable level of certainty, as in "if the victim was mutilated, the perpetrator is most likely disturbed." Steps in the scientific method of investigation include:

- Identifying the questions and define the key variables.
- Specifying the simplifying assumptions.
- Formulating a hypothesis.
- Testing the hypothesis with data.
- Retesting the hypothesis with additional data to validate.

Question No 22. How successful Investigation is performed? Also explain the steps of Investigation process.

Ans:

Guidance for Conducting a Successful Investigation

1. Do not 'go it alone' if you can avoid it. Good investigation requires discussion and it is all too easy to agree with yourself! Different type's people see things from different perspectives and in investigation you want to make use of this.

2. Remember to think things through before you begin. Do not rush in to interview witnesses or walk the site until you have decided what should come first and who is going to do what.

Gather your thoughts. Discuss with your 'team.' Find witnesses and make arrangements to interview them properly. Decide carefully when you will do the various necessary tasks.

3. Organise who will be responsible for all the information you will collect and which you will need for your analysis. If this is yourself, then set up a simple but effective system for storing and keeping it safe. Make sure none of your data is lent out or left lying around.

4. Set up your 'investigation headquarters' right away. This may sound 'over the top' but it isn't; you need somewhere to put up your Storyboard and Analysis charts so that you can come back to your investigation each day in an orderly way. Even small incidents or near misses (hits) could have been much bigger events; the reason you are investigating is to identify actions which could prevent a much more serious occurrence. Your investigation is extremely IMPORTANT no matter what size the incident.

5. As you gather your data, put it right away onto Post-its and then the Timeline chart. That way you can see in front of you what is emerging. And you can discuss your findings so far with your colleague/team. Using Post-its like this allows flexibility; nothing is fixed. You can move them around– or take them off the chart altogether.

6. Make sure that everyone feels able to input information. TOP-SET® has 'difference' at its core. Make use of this. Be open and accepting. What seems obvious is rarely the answer.

7. Do not discount the apparently naive idea. The non-expert too can have a very valuable contribution just because they can see with fresh eyes. Is there anyone in your office/establishment whom you have not thought of who could contribute well to the investigation?

8. Arrogance and bullishness have no place in investigation; each individual has equal value in this process. Often the quieter individual, the one who is listening, comes up with the gem.

9. Listen to others. Sometimes someone else's idea triggers something in your own mind. It's OK to piggy-back on the ideas of others.

10. Be open minded; it is dangerous to be fixated on any idea. Use the TOP-SET® indicators to direct you in different directions. Allow them to stimulate your own thinking. Remember, you are looking for truth, not convenient coat-hangers. And sometimes you just have to live with uncertainty. A good investigator can do that and can base their recommendations on what they have found without needing A SINGLE ANSWER.

Steps for Investigation process

Planning

Effective planning is a key component of any successful investigation: it will help you define the parameters of your investigation and keep you focused on what is relevant. We recommend drawing up a standard investigation plan at the start of every investigation, capturing the key issues and structuring your actions.

Of course, you cannot ever predict with certainty what direction an investigation will take.

During the course of the investigation, you may uncover issues that require further research and consideration, and could result in significant revisions to your plan. Even so, a good initial plan will help to reduce the disruption of unforeseen circumstances and keep your investigation focused.

The sample plan at the back of this guide might give you some ideas. At its most fundamental, the plan should include the following sections.

The allegation

A good investigation plan starts with a precise definition of the allegation. Knowing exactly what you are trying to establish will help you focus. Ambiguity about the exact nature of the allegation may cause difficulties later on in the investigation.

If you need clarification on any facts of the allegation you can approach the complainant.

You are required to tell the complainant that you have received the matter for local investigation, so this might be a good time to check any details

Relevant parts of the Code

It is useful to list the parts of the Code of Conduct that may have been broken, to help you focus the investigation in the right areas. We have found that one of the greatest dangers is becoming distracted by issues that only serve to muddy the waters and increase the amount of time and effort spent on an investigation.

Information

The complaint sometimes comes with a great deal of documentary information which you will need to sift through, recording the relevant parts on your plan.

From this, you should be able to work out what further information or evidence is needed to determine whether the alleged conduct occurred. Be as focused and precise as possible: being clear about what you need to know at this stage will help you avoid delays and distractions later on. You may find it helpful to produce a checklist of the elements that need to be proved.

Action plan

Set out how you intend to obtain the information you need. Your plan should include the witnesses you intend to interview, the order in which the interviews will be conducted, the questions you need to ask and the areas you need to cover. It should also include any documents, you need to obtain and any site visits you think would be useful.

It is usually best to secure all relevant documents before beginning the interviews as they may have an impact on the questions you want to ask. You should also consider what documents if any, you may wish to give to the interviewee before the interview.

Resources and targets

At this stage, you should have a reasonable idea about the resources needed to complete the investigation, such as time and expenses. Record them on your plan and make sure they are available to you.

We also recommend that you include target dates for completion of the various stages of your investigation and an overall target date for completion of the final report.

Establishing facts

In the vast majority of investigations, you will need to gather documents and conduct interviews to establish the facts of a case. This section considers how to go about it.

Gathering documents and background information

You will need to obtain the background information and other documentary evidence you have identified as relevant to the investigation. You may also wish to get written statements from witnesses, although these are usually only successful where the information you are seeking is very straightforward. They will not be helpful where you need to probe the answers given for further information, test an individual's responses, or where there is some doubt about the credibility of an individual's account of events.

Requests for information should:

- be made in writing
- explain the reasons for your request
- be precise about the information you need
- set a deadline for responding

You may wish, at this stage, to ask people to let you know if they are likely to be late responding. Ask them to explain any delays and agree a new deadline. It may also be helpful to give a copy of the letter to your chief executive, in case you need their help persuading people to co-operate.

It's important you contact anyone who missed the deadline straight away to ask them when the information will be provided. Do not accept vague promises; insist on a precise date. You may even want to offer to have it collected and agree a date and time for this.

Getting information from your own authority and other local authorities should be quite straightforward. These bodies have a statutory duty to provide the information you require and ethical standards officers are unlikely to refer cases to you for local investigation if they believe you will need information from other sources.

Conducting interviews

You should already have identified the people you need to interview and the areas you need to cover for your investigations plan, and considered the order in which they should be approached.

As a rule, you should plan the order of your interviews so that each witness is interviewed only once, although repeat interviews are sometimes unavoidable.

Interviewing the member who is the subject of the investigation first may save you a lot of time if, for example, they admit to the alleged breach of the Code of Conduct. It may also help you establish which facts, if any, are disputed. However, you may learn things during other interviews that you need to discuss with the subject member, requiring a second interview. If you think this is likely, you may wish to leave the subject member's interview until last. Alternatively, to help manage the subject member's expectations, you could explain at the start of the first interview that there may be a need for further interviews.

You also need to consider whether to conduct the interview in person or over the telephone. With face-to-face interviews, you should agree a time, date and venue for the interview in advance, and confirm these details in writing. You can also use this letter to remind members being investigated that they may wish to have legal representation, and advise interviewees if the interview is to be recorded. Some interviewees may prefer to be accompanied by a friend or colleague. This should not present a problem as long as the companion is not connected with the investigation in any way — for example, someone the member is accused of trying to secure an advantage for.

For telephone interviews, people may be happy to talk when you first call, but you should realise that it might not be convenient or they may need time to prepare. It might also be seen as unfair to spring an interview on someone without warning. Always check with the interviewee first, and where appropriate agree a convenient time to call them back. Ensure you keep the appointment as punctually as you would a face-to-face interview. Again, it might be a good idea to confirm the details of the interview in writing and explain if it will be recorded.

Recording interviews

If you intend to tape record an interview, you must ask permission of the person being interviewed in advance of the interview. You should never start to record and then ask permission. Once you begin recording, we recommend you get the interviewee to confirm for the record that they have given their permission to be recorded.

In face-to-face interviews, you may wish to ask a colleague to take notes for you if you are unable to record it. This will enable you to maintain eye contact with the interviewee and concentrate on their responses to your questions. The interview will also take a little less time. For telephone interviews, you might want to consider using a headset to keep both hands free for taking notes.

At the end of an interview, the interviewee should be offered a copy of any tapes made and told that they will be given the chance to approve or dispute the transcript or notes of the interview. We recommend you supply the tape straight away unless you have a specific reason not to — for example, if you are concerned it may be passed to other interviewees or the press. All statements should be confirmed promptly with the person who gave it, while the interview is still fresh in their mind.

Confidentiality

The statutory guidance asks you to treat the information you gather during an investigation as confidential, to ask interviewees to maintain confidentiality, and remind members of their obligations around confidentiality under the Code of Conduct. We suggest you do this both before and after the interview. However, it should be made clear to the person you are investigating that they are allowed to discuss the case with a friend, adviser or solicitor.

Evaluating

You need to review all the evidence you gather to determine if there are any gaps in it.

You must be able to take a view on all disputed relevant matters. Absolute certainty is desirable, of course, but not necessary. It is sufficient to form your opinion based on the balance of probabilities. If you cannot do this, you may need to seek further information.

You then need to weigh up all the evidence and decide if the alleged conduct occurred.

Again, you do not need absolute certainty — it is acceptable to come to your conclusion based on the balance of probabilities. If you decide that the subject member acted as alleged, you will need to consider whether his or her conduct involved a failure to comply with the Code of Conduct.

Reporting

When you have concluded your investigation, you need to write up your findings in a report to the standards committee. The statutory guidance includes detailed advice on this aspect of the investigation process but key points are summarised here.

You have the option of producing a draft version of your report first, giving key parties opportunity to review and comment on your findings and enabling you to check facts and ensure all aspects of the case have been explored sufficiently. A draft report may be particularly suitable if the facts are complex, ambiguous or disputed, or if the parties expect one. But it is not always necessary, and going straight to a final report will save considerable time.

Draft reports should be sent for comment to the complainant and the member who is the subject of the allegation. Ordinarily you should not need to send the draft to other witnesses or parties interviewed but you should have confirmed their statement. However, there will be occasions when you will need to disclose extracts of a draft report to any potential witnesses, especially if the report is critical of their actions.

Members may respond in whatever manner is most convenient for them. Responses to your draft may reveal the need for further investigation, or they may add nothing of relevance. There may

be occasions when responses reveal a need for further investigation and result in such significant changes to the report that you may wish to consider whether to issue a second draft.

Once you have considered whether the responses add anything of substance to the investigation, you will be able to make your final conclusions and recommendations. For more information on producing reports and directions on issuing your final report, refer to the statutory guidance.

Confidential information

Before issuing draft or final reports, consider whether the report contains any confidential information that should not go into the public domain, such as financial or medical details.

All information of this kind should be deleted from any copies of the report before they are made public. Your authority will be able to advise you further on this process, known as redaction.

Question No 23. Interview is considered more effective in investigation. How interview should be conducted for investigation. Which techniques are more useful to gather evidence while interviewing?

Ans:

Interviewing Witnesses.

The purpose of the interview is to:

- Find out what the witness has experienced.
- Establish a preliminary direction for the investigation.
- Complement other phases of the investigation.

Interviewing a witness is one of the most challenging tasks of an investigator. Skilled interviewing is an indispensable investigative tool. This process is not as simple as asking witnesses to relate everything they know about their encounter with an unexplained phenomenon at o-dark-thirty on the night of such and such. A cornerstone of successful interviewing is the awareness that a typical witness description comprises error-prone perceptions during the event and (unintentional) selective recall thereafter. The professional interview is usually the best single method of ferreting out the truth of the matter.

Witness statements and physical evidence go hand-in-hand and each may complement or clarify the other. Investigators may not realize the importance of seemingly innocuous testimony for days or even weeks after it is taken. Therefore, testimony obtained from witnesses should be as complete and detailed as possible.

Many factors influence, distort and limit information flow. When the investigator understands and practices effective interviewing techniques, the results of each interview can dramatically increase, in both the quantity and the quality of information obtained. Witnesses come in all types. Most will be honest and even helpful. Some will lie. Others will not want to become too involved. People all have differing abilities to remember and articulate what they observed.

You may meet individuals who are obnoxious, neurotic, dull or nervous. They cannot all be treated the same way. As an interviewer, you must develop personal techniques for maximizing the completeness and reliability of information sought from so many different kinds of people.

When to interview

You must act quickly. To maximize the likelihood of obtaining reliable information, interviews should be conducted early in your investigation, as close to the event as possible. As time passes, chronological and inferential confusion increases. The human mind has a tendency to fill gaps in recollection through logic or filling-in based on their own experiences. The longer witnesses have to reconsider events, the more they tend to do this. Keep in mind the possibility that their description of what they saw might change once they have time to reflect and their second impressions probably will not be as useful as their first.

You always should try to interview a witness at a time when he or she has the fewest competing time demands. The witness has more important ways to be spending their time. Interview witnesses at their convenience, not yours.

Prepare for the interview

Without adequate preparation, valuable time is spent in familiarizing oneself with the circumstances and deciding what questions to ask. The result may be a wasted discussion that omits essential items. A prepared investigator has a game plan to keep the interview on course and explore every possibility. Make a list of topics you want to cover. Write your specific questions down before the interview, but be prepared to take a different path of questioning, if necessary.

Generally, some information about the case is available beforehand, either from the witness directly or from a referring party (newspaper article, police agency). Before embarking on the interview, if at all possible, contact the reporter or police to determine whether anyone else reported the same event and obtain pertinent impressions of the witness when the initial contact was made.

Interviews should be conducted by prior appointment when possible. It is rude to just show up and expect the person to give you their time.

Interviewing by telephone

If you are really shy, interviewing by phone offers some advantages over in-person interviewing, because the person you are interviewing can't see your nervousness. You can make use of notes to guide you and help you through the questions.

That being said, when interviewing in person, you have the advantage. The person you are interviewing will find it harder to refuse you in person. Turn on the charm. Project your winning personality. When interviewing "one-on-one," you will have more time to state your case.

Professional appearance and behavior

The first rule of interviewing is punctuality. Never keep any witness waiting.

Be aware of your personal appearance and grooming. If you want people to believe that you are a professional investigator, consider every detail: dress, demeanor, and manner of speech. Act like a professional. Be a professional. Think before you speak! Decorum, politeness, and attentiveness are those qualities that seasoned investigators exhibit. Demanding and overbearing individuals can expect little cooperation.

Be friendly and courteous. Never forget that witnesses are giving you their valuable time.

Your notebook

_____Number the pages of your notebook.

_____Use pen, not pencil.

_____Write legibly.

_____Stroke through a mistake and initial it.

_____Do not rip out or skip pages.

_____Do not destroy notes.

_____Keep your notebook secures.

Interviews are not interrogations

An interview is an informal meeting where the interviewer approaches the witness on equal terms and encourages their cooperation, allowing them to relate observations without interruption or intimidation. An interrogation implies questioning on a formal or authoritative level, such as a lawyer-to-witness situation or a police officer-to-suspect session. Witness interviews must never have the feel and appearance of being interrogations. If witnesses refuse to cooperate in any way, they must not be harassed.

Separate the witnesses

Independent witness statements can corroborate other evidence in the investigation.

Keep witnesses to the same incident separated while waiting to interview them. Witnesses should not hear other accounts because they may be influenced by that information and mentally fill in parts of their observations based on what someone else may have seen or heard. It also may be helpful to ascertain whether witnesses have spoken with each other about the incident prior to being separated.

While the witnesses are waiting for the interview, keep them busy outlining the sequence of events or making a sketch of what they saw. Both assignments will help the witnesses remember important information about the event.

Never confuse your sources of information. Use a new page of notepaper for each new witness. Don't compare the prior testimony from previous witnesses with what the current witness is telling you during the interview.

Set up a private interview space

Select an environment that minimizes distractions while maintaining the comfort level of the witness. A comfortable witness provides more information. It might be helpful to designate someone to keep people from knocking on the door, to answer the phone, and ensure that physical distractions are minimized. Distractions will interrupt the memory retrieval. In addition, the interviewer can encourage the witness to block out these distractions by closing their eyes

and concentrating on the memory. Secure all necessary items and resources prior to the interview.

Avoid interviewing the witness in an environment where such distractions are more likely to occur, such as a place of business. This should be determined with the witness to accommodate their schedule and needs.

Consider using a tape recorder

In order to make sure that you have all the facts, consider recording the interview. The inconspicuous size and simplicity of the micro-recorder is perfect for this purpose.

You must have the permission of the witness to record the interview.

Getting permission is not always easy. One approach to acquiring permission to record the interview is do not make a big production out of it. Tell them that recording an interview is Standard Operating Procedure for investigations nowadays and that it helps things move along faster and ensures accuracy. It would really save you a lot of trouble by not having to scribble page after page of handwritten notes.

Once you have their permission to record, state the following items at the beginning of the recording:

_____Your name and your role as investigator.

_____Date, time and location where the interview is taking place.

_____State the witness's name and address and indicate that they have given you permission to record this conversation for the sake of accuracy. "Mrs. Mabel Smith, you are aware that we are recording this interview and I have your permission, is that correct? A nodding of the head can't be heard on the tape. Make sure the witness verbally answers this question with a "yes."

_____Indicate the subject matter of the interview.

The interviewer should point out that he or she would also be taking brief notes, in case modern technology fails to do its part. After a few minutes of conversation, the tape recorder should be

rewound and played back to check the quality of the recording. The witness now has an opportunity to hear himself or herself and hopefully feel reassured that they will not be misquoted as these machines do their work during the interview.

Interview stage 1: mutual evaluation and building rapport

The first stage of an interview can be called mutual evaluation.

Give the witness a chance to relax. A few minutes of small talk will help break the ice and build rapport. Lean forward to emphasize interest in what they have to say. Maintain eye contact. Ask them some routine questions for basic information. Get the correct spelling of their name and then refer to the witness by name and listen effectively. You can get the answers to these simple questions elsewhere, but people enjoy talking about themselves and it shows you want to get all the facts correct.

If you conduct the interview at the home of the witness, survey your surroundings immediately. People surround themselves with symbolic items of interest or importance in their lives. Look around to find some common ground or interesting hobby the witness has. Get them to like you. Show understanding and concern. Establish a bond of trust and become their friend. Offering a sympathetic, non-judgmental ear to someone who needs to be understood, will often trigger a flood of information. The interviewer should treat the witness as an individual and not as a statistic.

Always completely explain who you are and the purpose of your investigation. It usually is appropriate to take this time to make sure the witness understands the ground rules of the interview --- how long it will probably take, its confidentiality, and what its purposes are. Always respect requests for anonymity.

- Witnesses may be more open if only one investigator is present.
- If two investigators conduct the interview, be sure only one asks questions at a time.
- It is prudent to have a third person in the room if the investigator and witness are of opposite sexes or if the witness is a child.

- ❖ All requests for a third party to be present during any interview must be honored.
- ❖ Never ask a single question about the event before the formal interview begins.

Effective listening and investigator bias

The value of any interview depends on many things. The investigator has control over some factors that appear to have an effect on interview success: the time and place of the interview, the number of interruptions, the scope and wording of questions, and effective listening skills.

The most important thing about listening that any investigator needs to know is that there is a vast difference between hearing and listening. Most of us prefer to talk rather than listen and are able to listen about four times as fast as the other person talks. There is a danger that leaping ahead, trying to anticipate what will come next, and not paying attention to the testimonial evidence may fill this gap. One of the biggest consequences of poor listening habits is a shallowness of understanding.

Listening is more important than talking. An active listener shows respect for what the witness is feeling and expressing. There is a basic but powerful need to be understood and the investigator who is also a good listener is filling that requirement in addition to gaining necessary information.

Effective listening begins by keeping the mouth tightly closed.

We are all biased. Everyone has preferences and beliefs.

Investigator bias refers to the process by which the investigator influences the interview. When your preferences and beliefs intrude into the interview, they are likely to produce erroneous information.

The behavior of the investigator when asking questions and recording answers affects the flow of information. Your act of jotting down an answer or not jotting it down may cause the witness to believe the subject is important or unimportant, causing them to expand on or stop talking about the topic. If you communicate, either verbally or nonverbally, that some facts are unimportant or that you do not believe what the witness is telling you, that witness is likely to stop offering vital

information. Studies show that even the particular words you use, the way you phrase a question, or the sequence in which you ask questions can alter the way in which a witness remembers an event.

Be prepared to drop the filters that get in the way of effective listening. It is imperative that you become free enough of your own agenda to really hear someone else.

Bias is also introduced by investigator reaction to witness testimony. What ends up in your memory may not be what they told you. You may simply not hear some things that the witness might say, especially if those things run counter to your own attitudes, beliefs, opinions or preconceptions. You may edit an answer and store the characterization in your memory. Be sure to differentiate between what the witnesses say and how you hear and interpret their testimony. Any preconception as to the actual nature of a given report makes an investigator highly susceptible to errors in gathering the evidence.

Interview stage 2: the narrative overview

The investigator needs the witness to report the event in more detail than would be conveyed in normal conversation. The investigator should explain this need for detail to the witness to ensure the witness is fully aware of how to provide the description.

The second stage of the interview is to obtain a recollection of the events in narrative form, without interrupting to ask for details. Remember that this narrative overview provided by the witness, while not likely to be very complete, will be highly accurate. During this stage, your job is to listen, not to talk. You should encourage the witness to talk, facilitate communication, and be careful not to influence inadvertently what the witness thinks is important. It is probably a bad idea to take notes at this stage, since they distract you from listening and may subtly influence the conception of what is important. This phase will provide you with a summary of the event and an outline of issues to pursue in detail later in the interview.

Allow an articulate witness to talk without interruption. This helps the witness relax, bolsters self-esteem, and facilitates communication. Interrupting the mental images of the witness risks the dilution, contamination or loss of the original mental image or memory forever.

Not all witnesses will spontaneously pour forth a long narrative of facts upon merely being asked to tell what happened. Some may be reluctant or shy. You will have to take an active role by encouraging communication with subtle techniques that will stimulate the witness to talk without influencing the content of what is said such as:

Noncommittal encouragement includes head nods and brief remarks such as "uh huh," "really," and "I see."

There is a natural tendency to fill silence in with more conversation. You must be careful not to immediately jump into gaps in conversation with questions. If you let the silence continue, the witness will probably start talking again. Care must be exercised not to overuse silence because it may embarrass a witness who cannot think of what to say next.

Offer neutral questions such as "Can you think of anything else?" and "What else happened?"

During this crucial stage, your questions must not contain leading topic suggestions.

Interview stage 3: detailed chronology

After the witness has completed the narrative overview, you will want to probe more deeply for details. In order to minimize chronological confusion, you should go back over the events in chronological order. To do this, you first must identify the point at which the chronology should begin. In some interviews, the starting point will be obvious. You still must verify that this is the first relevant event, but that will be easy to do by a question such as, "Can you think of anything that happened before the incident?"

In other situations, determining the chronological starting point may be more difficult. One inhibitor to communication is perceived irrelevancy. If a witness has rejected earlier events as irrelevant or inconsequential, that person may not mention them during the overview stage, and will be unlikely to volunteer them if asked whether anything relevant happened earlier. A witness to a traffic accident may think that the sight of a speeding car is the first relevant event. If you accept this, you may miss out on crucial events that happened earlier --- the witness may have heard the sound of brakes, seen a man on the corner who will turn out to be a valuable

eyewitness or overheard the owner of the car say that the brakes were bad the day before the accident.

Once you have obtained an overview of the problem from the witness, and have ascertained the starting point, it is time to probe for details. In most cases, a straight step-by-step chronological order will maximize the completeness of the information. Taking notes usually is recommended during this phase, since particular important details, such as the names and addresses of other witnesses, are difficult to remember accurately. During this stage, you must take control of the tempo and the scope of detail of the interview, preventing the witness from jumping ahead, and probing for details. This is known as topic control.

This is when you use the "funnel" sequence of questions, from broad to directed to narrow. During this part of the interview, in which you are seeking more detail, two probes are commonly used:

A request for elaboration may take several forms. First, elaboration might imply a need for continuing the "story" or finishing the trend of thought. This would include such probes as: "Then what happened?" or "What happened next?" Second, the elaboration might not imply a "moving on" with the story, but merely requests the respondent to say more about the topic at hand. For example: "Tell me more about that." or "What else could you say about that?"

The clarification probe not only asks for more information on the topic under discussion, but it also specifies the kind of additional information that is needed. A request for clarification may take many specific forms of two general types. First, the interviewer might request a more detailed sequence of events, beginning at a certain point in the action described in the immediately preceding response. Second, the interviewer might probe for more detailed information on some specific aspect, rather than some particular period of time.

Good questions, bad questions

Ask your questions clearly.

Experienced interviewers never read their questions. The questions blend into the conversation. As the interview progresses, your notebook becomes important. Additional questions may come to mind that can be jotted down for inclusion when the moment is appropriate. Reminders of promises made should also be written down, so that they can be kept rather than forgotten, once the interview is over.

Ask specific, thought-provoking questions. Avoid asking questions that require just a YES or NO answer.

Avoid interrupting the witness. Ask only one question at a time. Let the witness complete each answer before you go to another question. If you interrupt an answer, you may communicate that you think the matter unimportant. Interrupting the witness during an answer discourages the witness from playing an active role and disrupts their memory. Rather than interrupt, the investigator should discreetly make a note and follow up at a later time with any questions that arise.

Do not immediately continue questioning when a witness pauses after an answer. It is important to allow for pauses after the witness stops speaking and before continuing to the next question. During a pause, the witness may be collecting their thoughts and could continue to provide valuable information, if provided ample time.

Tailor your questions to the witness. Because the witness, rather than the investigator, possesses the relevant information, the witness should be mentally active during the interview and generate information, as opposed to being passive and waiting until the investigator asks the appropriate question before answering. The investigator can encourage the witness to be mentally active by asking open-ended questions and then following up with nonleading, closed-ended questions.

An open-ended question allows for an unlimited response from the witness in his or her own words: "Tell me in your own words what happened."

Open-ended questions allow the witness to play an active role, thereby generating a greater amount of unsolicited information. Open-ended responses also tend to be more accurate and promote more effective listening on the part of the investigator. The investigator also is less

likely to lead the witness when framing questions in this manner. However, open-ended questions are not adequate by themselves because they seldom provide enough detail.

Open-ended questions:

_____Make no suggestions

_____Invite witnesses or victims to talk in their own words

_____Act as memory prompts

_____Get people talking

_____Encourage full answers

_____Help to get accurate information

A closed-ended question, in contrast, limits the amount or scope of information that the witness can provide: "What color were the creature's eyes?" Although it is preferable to use open-ended questioning, the investigator should follow with more directed questions if the witness is unresponsive to open-ended questions or provides imprecise responses.

Closed-ended questions:

_____Suggest an idea to the witness or victim

_____Lead the witness or victim to repeat what you said

_____Take one word to answer

Information should be gathered using primarily open-ended questions. More specific, closed-ended questions should be used only when the witness fails to provide a clear or complete response.

Leading questions suggest an answer and may distort witness perception or memory: "Did the creature have glowing red eyes?" The investigator needs to determine only what the witness knows, uninfluenced by what the investigator might expect or know from other sources:

Avoid trick questions or other tactics that puts the witness in an unfriendly mood.

More interview techniques

Encourage the witness to volunteer information without prompting. This allows the witness to maintain an active role in the interview. Unprompted responses tend to be more accurate than those given in response to an interviewer's questioning are. Use a structured format (fill-in-the-blank sighting report form) as a last resort and only after you have collected as much information as possible from all open-ended and close-ended questions.

Encourage the witness to report all details, even if they seem trivial. If the witness does not believe that certain information is relevant, he or she is not likely to offer it, and the witness may not give serious consideration to the answer even if asked. All of the information that the witness provides is important.

Caution the witness not to guess. Witnesses may guess in an attempt to please the interviewer. Instruct the witness to state any uncertainty they may feel concerning an answer.

Ask the witness to mentally recreate the circumstances of the event. Recreating the circumstances of the event makes memory more easily reached. Instruct the witness to reflect about their thoughts and feelings at the time of the incident.

Encourage nonverbal communication. Some information can be difficult to express verbally. Witnesses may have a very good memory of the incident, but fail to communicate the knowledge effectively. The interviewer should try to facilitate the conversion of memory into effective communication. Encourage the witness to draw rough sketches and diagrams or to use gestures to demonstrate actions.

Volunteer no specific information about the case. Telling any witness facts about the case may influence their memories of the incident. The interviewer must ensure that information from the witness is based only on memory and not on any information gained from other witnesses or other aspects of their investigation. Prompting and leading questions are easy traps to fall into and must be avoided.

If the witness brings up the name of someone new to the investigation, make sure you write down the name and then interview the new witness.

Interview stage 4: concluding the interview

The final stage is to end the interview. A poorly handled farewell can destroy the rapport you have built up during the interview.

In general, you should:

Summarize the main facts for the witness to verify.

Always thank the witness for their cooperation. This reinforces the rapport that has been developed and your commitment to the witness, thus encouraging the witness to continue to cooperate.

Set an agenda for future meetings and obligations. Be specific.

Encourage the witness to contact you if they remember any more details. Witnesses will often remember additional, useful information after the interview. Remind the witness that any information, no matter how trivial it may seem, is important. Make sure that they have your phone number or other pertinent contact information. Maintaining open communication channels with the witness throughout the investigation can lead to additional information and evidence.

After the interview

Immediately (at your first opportunity) write up a report containing everything you learned in as much detail as possible.

All reports should indicate the persons present during interviews, and their status.

Point-by-point consideration of the accuracy of each element of witness testimony can assist in focusing the investigation. This technique avoids the common misconception that the accuracy of an individual element of description predicts the accuracy of another element:

Consider each individual component of testimony separately. A witness may not have knowledge about all elements of an event. Some recollections of observations may be correct, while others may not.

Review each element of testimony in the context of the entire statement. Look for inconsistencies within the statement. Note any inconsistencies for future reference. Also, note that the inconsistency of one element with another does not mean that the entire statement is inaccurate.

Review each element of testimony in the context of evidence known to the investigator from other sources. Note any inconsistencies between the witness statement and other information. These inconsistencies can be useful in assessing the accuracy of elements of witness statements as well as in directing the investigation.

Multiple, mutually corroborating witnesses greatly aid in resolving ambiguities. When multiple witness statements are numerous or contradictory, they can be more objectively examined by preparing a matrix, with witnesses listed on one axis, and information provided on the other. Associating multiple witnesses with the information they have provided allows a check on their credibility against others that provided similar or conflicting information. This method has the added benefit of allowing investigators to examine the frequency with which a given item of testimony recurs.

Follow-up interview

Many investigators prefer to conduct a follow-up interview of the witness at the scene of the experience. This can be beneficial since the witness may be able to point out or remember more details because of the surroundings. It can also give the interviewer a better understanding of the sequence of events. Attempt to recreate the events if possible. Place each witness in the same position they were in when the event occurred.

Canvass the area for other witnesses

Witnesses may always be reluctant to come forward for any number of reasons. Other persons in the vicinity, such as neighbors, may have heard or seen something that could assist in your investigation.

Go door-to-door in the immediate vicinity of an event.

Introduce yourself matter-of-factly and politely ask this open-ended question:

"Have you seen or heard anything that is out of the ordinary?"

Tell the neighbors as little information as possible and never reveal your primary source. Nothing can destroy your effectiveness as an investigator more quickly than for word to spread you are giving information to people you promised the witness you wouldn't.

If a neighbor reports something relevant, take a detailed statement.

Question No 24. What is Computer Forensic?

Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems.

If you manage or administer information systems and networks, you should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and

presenting evidence to the courts. (The word forensics means "to bring to the court.") Forensics deals primarily with the recovery and analysis of latent evidence.

Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive.

Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal "scientific" discipline. We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

Question No 25. Why is Computer Forensics Important?

Adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure. You can help your organization if you consider computer forensics as a new basic element in what is known as a"defense-in-depth"1 approach to network and computer security. For instance, understanding the legal and technical aspects of computer forensics will help you capture vital information if your network is compromised and will help you prosecute the case if the intruder is caught.

What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected. Recent legislation makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data.

Computer forensics is also important because it can save your organization money. Many managers are allocating a greater portion of their information technology budgets for computer and network security. International Data Corporation (IDC) reported that the market for intrusion-detection and vulnerability-assessment software will reach 1.45 billion dollars in 2006. In increasing numbers, organizations are deploying network security devices such as intrusion

detection systems (IDS), firewalls, proxies, and the like, which all report on the security status of networks.

From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

What are some typical aspects of a computer forensics investigation? First, those who investigate computers have to understand the kind of potential evidence they are looking for in order to structure their search.3 Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. Second, the investigator must pick the appropriate tools to use. Files may have been deleted, damaged, or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process.

Two basic types of data are collected in computer forensics. Persistent data is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off. Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it.

System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

Question No 26. Forensic Computer is a difficult task. Discuss the process to conduct Cyber forensic.

Ans:

The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual

reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found.

Let's break this definition down.

Preservation

When performing a computer forensics analysis, we must do everything possible to preserve the original media and data. Typically this involves making a forensic image or forensic copy of the original media, and conducting our analysis on the copy versus the original.

Identification

In the initial phase, this has to do with identifying the possible containers of computer related evidence, such as hard drives, floppy disks, and log files to name a few. Understand that a computer or hard drive itself is not evidence - it is a possible container of evidence.

In the analysis phase, this has to do with identifying the information and data that is actually pertinent to the situation at hand. Sifting through Gigabytes of information, conducting keyword searches, looking through log files, etc.

Extraction

Any evidence found relevant to the situation at hand will need to be extracted from the working copy media and then typically saved to another form of media as well as printed out.

Interpretation

This is a biggie. Understand that just about anyone can perform a computer forensics "analysis." Some of the GUI tools available make it extremely easy. Being able to find evidence is one thing, the ability to properly interpret it is another story. Entire books could be written citing examples of when computer forensics experts misinterpreted their results of a forensic analysis . We'll cite one example.

The experts for the prosecution in a case used a popular GUI tool that came with a script for finding Internet search engine activity. When they ran the script, they found literally hundreds

and hundreds of "searches" that supposedly had been conducted by the defendant. Therefore, the defendant had intentionally accessed certain types of information related to these searches - the searches showed intent.

When the experts for the defense examined the same evidence, they realized that each and every one of these "searches" was actually a hyperlink and not a search at all. The hyperlinks were formed in such a way that when a link was clicked, a database was searched to pull up the most current information related to the link. The way that the links within the page were formed was what the GUI tool honed in on, as they were formed similarly to fragments and Web pages that could be found to indicate search engine activity.

The experts for the prosecution took for granted that their automated tool was accounting for any variables, and would only show them searches that had actually been conducted. A big mistake. Theses experts lacked the technical skills to authenticate their results, so they depended entirely on a single automated tool.

This leads to a very important lesson. Results from any tool should always be thoroughly checked by someone versed in the underlying technology to see if what appears to be a duck is actually a duck.

In the very same case, the experts for the defense recovered reams of email that the prosecution experts did not find. This was due to the fact that the prosecution experts simply did not know how to find it.

It is interesting to note that both the experts for the defense and the prosecution used the same primary tool in their analysis. The differences in what was found by one side versus the other, as well as the differences in interpretation was due to the experience and education levels of the experts - it had nothing to do with the tool being used.

Documentation

Documentation needs to be kept from beginning to end, as soon as you become involved in a case. This includes what is commonly referred to as a chain of custody form, as well as documentation pertinent to what you do during your analysis. We cannot overemphasize the

importance of documentation. When involved in a situation where you are conducting a computer forensics analysis, we recommend that you establish and keep the mindset that the case or situation is going to end up in court. This will go a long way in helping you to make sure that you are keeping the appropriate documentation. Take for granted that you will be questioned on every aspect of the case, and everything that you do.

Rules of Evidence

There are various tests that courts can apply to the methodology and testimony of an expert in order to determine admissibility, reliability, and relevancy. The particular test(s) used will vary from state to state and even from court to court within the same state. Commonly, you will hear about the Frye test and the Daubert test. You need to be aware of the Rules of Evidence for your locale and situation. Your best bet is to ask legal counsel about any Rules of Evidence that you need to be aware of pertinent to the situation, and familiarize yourself with this information early on.

We recommend that you find and read the Federal Rules of Evidence on the Internet, and conduct searches using the terms "daubert test" and "frye test" as keywords.

Legal Processes

This has to do with the processes and procedures for search warrants, depositions, hearings, trials, and discovery just to name a few.

This can also be related to processes relevant to your employer, as well as conducting computing investigations internally for your employer.

If you are conducting computing investigations for your employer, the best advice we can offer is to work as closely as possible with legal counsel and those in your Human Resources department before and during a computing investigation. You'll not know everything you need to know when you start working in this field - it is a learning process.

Integrity of Evidence

This has to do with keeping control over everything related to the case or situation. We are talking about establishing and keeping a chain of custody, as well as making sure that you do not alter or change the original media. As well, you cannot talk to other people about the case or situation specifics that are not involved.

Factual Reporting of the Information Found

Your findings and reports need to be based on proven techniques and methodology, and you as well as any other competent forensic examiner should be able to duplicate and reproduce the results.

Providing Expert Opinion

You may have to testify or relate your findings and opinions about your findings in a court of law or other type of legal or administrative proceeding.

Two Primary Types of Computer Forensics Investigations:

Computer forensics techniques and methodology is used in two primary types of investigations. The first is when the computer(s) was/were used as an instrument to commit a crime or involved in some other type of misuse.

The second is when the computer is used as the target of a crime - hacked into and information stolen for example. When computer forensics techniques and methodology are used in this situation to figure out what happened, we typically call this incident response.

In the first type of investigation, you may or may not be present when the computing device is shut down to begin an investigation. You may have hard drives and other media delivered to you to analyze.

In the second type of investigation, you will typically always want to capture information that is extremely volatile, such as information contained in RAM concerning network connections and running processes.

Regardless of the situation, and whether the evidence will be used in a court of law or as the grounds for a letter of reprimand, the techniques, procedures, and methodologies used should be largely the same.

What starts out as a letter of reprimand given to an employee for misusing company computing resources, may end up as a lawsuit against the employer.

What starts out as an investigation concerning Internet access at odd times may reveal that child pornography was accessed.

Question No 27. Explain the Computer Forensic Examination Process in detail.

Computer forensics involves the preservation, identification, extraction, interpretation, and documentation of computer evidence. The field of computer forensics has different facets, and is not defined by any one particular procedure. At a very basic level, computer forensics is the analysis of information contained within and created with computer systems, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved.

In many cases, the information gathered during a computer forensics investigation is not readily available or viewable by the average computer user. This might include items like deleted files and fragments of data that can be found in the space allocated for existing files, which is known by computer forensic practitioners as “slack space”. Special skills and tools are necessary to be able to obtain this type of information or evidence.

Typically, confirming or preventing a crime or violation through a computer forensics examination is a reactive measure to a circumstance. However, today, computer forensic examinations are often used pro-actively for the continuous monitoring of electronic media. In some cases, computer forensics is even used in a debriefing process for employees exiting a company.

Active, Archival, and Latent Data

In computer forensics, there are three types of data that we are concerned with - active, archival, and latent.

Active Data is the information that we can actually see. This includes data files, programs, and files used by the operating system. This is the easiest type of data to obtain.

Archival Data is data that has been backed up and stored. This could mean backup tapes, CDs, floppies, or entire hard drives.

Latent Data is the information that one typically needs specialized tools to access. An example of latent data would be information that has been deleted or partially overwritten.

A computer investigation could involve looking at all of these data types, depending on the circumstances. Obtaining latent data is by far the most time consuming and costly.

Computer forensics is all about obtaining the proof of a crime or breech of policy. It focuses on obtaining proof of an illegal misuse of computers in a way that could lead to the prosecution of the culprit.

The primary phases in a computer forensics examination are:

- Discussion of suspicion and concerns of potential abuse, by telephone
- Harvesting of all electronic data
- Identification of violations or concern
- Protection of the proof
- Confirming qualified, verifiable evidence
- Delivery of a written report and comments of the examiner

If you think you may have a problem, it is best to act quickly since computer evidence is volatile and can be readily destroyed. It is also better to know for certain than to risk possible consequences. If you are unfortunate enough to uncover a potential problem, it may be prudent to seek confidential advice from a Certified Forensic Examiner before determining a solution.

Handling this situation on your own is a risky strategy which may have far-reaching effects. If you are committed to using in-house staff, remember the basics of evidential integrity - and don't be tempted to use shortcuts.

When carried out correctly, the forensic analysis of computer systems involved in abuse can provide valuable evidence which might otherwise have been lost or overlooked. Performed incorrectly, and your evidence could give guilty parties the opportunity they need to get a case dismissed.

Steps in the Forensic Examination Process

Computer forensic investigations should always be conducted by a Certified Computer Forensic Examiner. They will use licensed equipment which prevents tainting of the evidence and ensures its validity in court. The steps involved for a computing investigation are briefly summarized below:

Step 1

A chain of custody is established. The examiner makes sure they are aware at all times where any items related to the investigation are located. A safe or cabinet is often used to secure items.

Step 2

All relevant information is cataloged. This includes active, archival, and latent data. Information that has been deleted will be recovered to whatever extent possible. Encrypted information and information that is password-protected is identified, as well as anything that indicates attempts to hide or obfuscate data. The integrity of the original media is maintained to the highest extent possible, which means that the original source of information should not be altered. An exact copy of a hard drive image is made and that image is authenticated against the original to make sure that it is indeed exact.

Step 3

Additional sources of information are obtained as the circumstances dictate. This includes firewall logs, proxy server logs, Kerberos server logs, sign-in sheets, etc.

Step 4

The information is analyzed and interpreted to determine possible evidence. Both exculpatory (they didn't do it) and inculpatory (they did it) evidence is sought out. If appropriate, encrypted files and password protected files are cracked.

Step 5

A written report will be submitted to the client with the investigator's findings and comments.

Step 6

If necessary, the investigator will provide expert witness testimony at a deposition, trial, or other legal proceeding.

The information contained in this document covers the basics, and really doesn't do full justice to all facets of computer forensics. However, you should now have a better understanding of what steps are involved in the process.

Conducting an Investigation of Computer Crimes

There are a number of reasons why an organisation might want to conduct an investigation that involves gathering computer evidence. Computer crime investigations can be different in scope and outcome than tradition investigations, but the evidence gathering techniques are the same. The same care and conduct should be used in an investigation involving the improper use of computer resources as in the investigation of specific violations of law. Computers are now such a part of our daily activity that it is only natural for them to be used as extensions of ourselves for all sorts of activities.

When conducting a computer-crime investigation, a primary consideration should be determining whether an outside forensic examiner is needed or whether the expertise is available in-house. This determination will depend, to a large extent, on the complexity of the examination required and whether the intended examiner is trained and experienced in forensic recovery, preparing legally sufficient reports, and testifying as a witness. Some organizations have invested in their own in-house personnel, whom they have trained and outfitted with the proper equipment and software tools to conduct the examination and analyze the digital evidence. Others have acquired and retained the services of an outside examiner as a disinterested third-party who will be able to conduct a thorough examination, prepare a proper report, and deliver expert testimony if needed in legal proceedings.

Another consideration involves determining that a crime has in fact been committed. If it is determined at the beginning of the investigation that a formal referral to a law enforcement or

prosecuting agency will be made, then the authorities must be before the investigation begins to determine whether law enforcement personnel should participate in the examination and analysis procedures or if the law enforcement entity is comfortable with the in-house personnel's level of expertise. In some jurisdictions, an examiner from the law enforcement community may not be available on short notice or at all.

Question No 28. Explain the difference between computer forensic and computer investigation.

Computer Investigation and Computer Forensics

There are several definitions and different schools of thought for this field of investigation, but all practitioners in the field will agree that investigations typically involve four phases: seizure, image acquisition, analysis, and reporting and testifying.

Seizure

In the seizure phase, it is important to understand who has the authority to seize the ~tal equipment as well as the proper methodology to use so that evidence is not destroyed or tainted.

Image Acquisition

The image-acquisition phase involves the use of decision making processes to determine the best method for acquiring an image of the suspect system and the proper use of software and hardware tools to facilitate the image capture. The examiner has to be sure that the image is created and preserved in a manner that will withstand a legal challenge.

Analysis

The analysis phase is arguably the most time consuming phase, especially for a financial crime or fraud investigation. This phase involves the use of specialized software designed to give the examiner the means to locate and extract ate facts that will be used as evidence in the

investigation. The evidence can serve to incriminate the subject of the investigation or it can be exculpatory by disproving the subject's involvement.

Reporting and Testifying

The reporting and testifying phase is where the hours of analysis are reported fairly and objectively. In this phase, a qualified computer forensics expert may be asked to render an opinion about the use or misuse of a computer system. This is where experience and training are tested and where examiners must know with certainty that their opinion is based on their research, knowledge, and experience and that an opposing expert will not find fault with their conclusions;

Each phase is dependent on the phases that come before it. For instance, if the seizure phase is handled incorrectly, then each of the following phases can suffer and ultimately render the reporting and testifying phase moot.

Each phase requires a degree of mastery before moving on to the next as one develops into a computer-forensic examiner. The analysis phase generally takes the longest amount of time to master. The seizure phase is one of the most critical of the process so we will focus primarily on it.

Computer Investigation Versus Computer Forensics

While at first these terms may appear synonymous, an important distinction exists between the two. An investigator leading an investigation into a crime that involves a computer is not necessarily and, in most cases, should not be the forensic examiner. Itisimportant to keep these areas separate. Combining the two, especially in cases in which the suspect is already named, invites questions about the objectivity of the forensic examination. It could also subject investigators to unwelcome scrutiny regarding whether they suppressed exculpatory evidence that may have been found during an examination by a more objective investigator.

Digital Evidence

Digital evidence, when boiled down to its basics, is simply binary data (ones and zeroes) that is interpreted by the computer. Everything that is digitally stored is made up of these ones and

zeroes, from the programs themselves to the data with which the programs interact. Interpreters built into the program show these ones and zeroes as hex code. This hex code is then translated onto the page or website seen on the computer screen.

As the professional use computer technology increases, so does the criminal use. Child pornography garners the bulk of computer-crime headlines, and it appears to be the crime investigated most often by law enforcement using computer evidence. However, financial crimes and frauds committed by use of computers are probably the most common types of computer crimes committed. The investigation of financial crimes generally requires a level of expertise not commonly held by a investigators; therefore, there is additional knowledge and experience required when conducting a forensic computer examination in a financial or fraud case. Most law enforcement computer examiners' experience is focused on child pornography investigations.

There are three types of situations in which computer evidence is generally discovered: (1) computers as the target of crime, (2) computers as the instrument of crime, and (3) computers as the repository of evidence.

Computers themselves can be the targets of crime. Crimes committed against computers include computer and computer component theft, system intrusions, software piracy, and software theft.

Computers can also be used to facilitate a crime. When this occurs, the computer is known as the tool or instrument of crime. In such cases, as one would expect, examiners commonly encounter computers that have been used in offenses such as the solicitation of minors in chat rooms, check fraud, and counterfeiting.

Generally speaking, in all computer investigations the examiner attempts to locate the storage of potential digital evidence, in one form or another, on the computer system. The computer system involved in the investigation is a potential repository of evidence whether the user intended to store an item or not. Therefore, the examiner is interested in incriminating evidence that the user intentionally or unintentionally stored on the computer system.

The proper handling of digital evidence is critical; it is easily altered or destroyed if handled improperly. The destruction of digital evidence through improper handling can result in a finding

of spoliation of evidence by a judge or can raise questions about the alteration of exculpatory evidence by the defence. .If a judge determines that the authenticity of the evidence cannot be satisfactorily made, then he may rule that the evidence is inadmissible.

Examiners should be aware that computer files can be altered simply through the normal.. startup process; Most of the Microsoft operating systems, such as Windows XP, change the time and date stamps on a number of rues during startup and delete a number of temporary files during the shutdown process. These pieces of information could be critical to the investigation.

Hardware

It is important for the examiner to understand and be able to recognize: various pieces of computer hardware so that he can decide whether he should seize a particular computer component. The examiner should be familiar with the various forms that digital evidence can take. Items used for digital storage have become so compact that it is now possible to store vast amounts of data on items that can fit in a pocket or attach to a keychain. In most cases these devices are smaller than a matchbook and are capable of storing anything digitally.

Examiners may only have one opportunity (especially in a legal proceeding, such as a search-warrant execution) to determine the items they need to seize. Because of this, examiners must be able to assess the hardware at the scene to determine its relevance to the investigation.

As mentioned previously, digital evidence can take many forms. Not all devices, however, are made so that an examiner can interface with the device to conduct an analysis. It is for this reason that it is important for the examiner to be familiar with the technology in computer forensics. For example, an entire subset *of* computer forensics has been developed in the area of cell-phone forensics, Smartphone forensics, and MP3/iPod forensics.

Examiners must also be aware of the latest advances in printer technologies. Many computer networks have installed printers with large hard drives the eliminate the need for a large print server. The printers themselves may now be the repository of additional evidence that at one time resided on a local machine or on a print server.

Question No 29. What are important cautions while going to seize Computer for investigation?

Considerations when Conducting the Seizure

There are a number of practical considerations and procedures to employ when the decision is made to go forward with a computer seizure. One of the primary considerations that is often neglected is the subject debriefing, when the subject is asked for passwords and whether any encrypted data exists on the target computer.

Procedurally, it is important to identify any destructive processes that maybe running on the machine before beginning the seizure. If such a process appears to be running, unplug the machine immediately.

Before beginning to disconnect the system, make certain to isolate it from any outside connections, such as a phone modem or a CATS network connection; another consideration to be aware of is a wireless connection, which may not be immediately apparent.

Be certain to document the scene with photographs or a diagram, depending on the complexity of the setup, remembering that it may be a year or longer before testimony about what the office looked like on the day of the seizure will be asked for in a !egal proceeding. Additionally, it is important to document what is on the screen if the system is on, as well as what processes are currently running. Many people have a habit of Writing down or recording their passwords near their computer, so examiners should look around for notes that may appear to be passwords. This practice may aid in the discovery of passwords needed to access encrypted data in the event the subject of the investigation is being uncooperative.

The second golden rule when securing a computer is, don't peek through the fues. This also applies to disks. If a system is running, the examiner may be tempted to click on the My Computer icon to look for evidence and/or copy filestoa flash or optical storage device. This should never be done, because each file the investigator touches will have its original time

stamps changed; once this is done the original time stamps cannot be recovered. It will be obvious to the forensic examiner that this has occurred.

There are two methods for shutting down a running system, a hard shutdown and a graceful shutdown. Generally, the hard shutdown is preferred. There may be extenuating circumstances that would lead the investigator to perform a graceful shutdown, so it is important to evaluate the best shutdown option based on the type of data being preserved and the possible ramifications of a hard shutdown based on the type of operating system installed. A hard shutdown is basically pulling the power cord from the back of the PC.

Laptop computers present additional considerations. When seizing a laptop, it is important to remove the battery first and then pull the plug. It is essential when seizing a laptop to recover all of the comp9nents that belong to the laptop such as zip drives, CD- and DVD- ROMs, and power supply. Often laptop computers must be imaged with their drives installed and because of the proprietary nature of the laptops themselves, they will only function with their own components.

Once a computer is seized, it is necessary to secure it in such a way that will allow the investigator to testify, if need be, that no unauthorized access to the suspect system occurred.

What Can the Computer Forensic Examiner Locate?

A computer-forensic examiner is a trained professional who is capable of analyzing digital media at the hexadecimal level. The hexadecimal level means that every sector and all the bytes in those sectors are available for viewing. This includes deleted files, both purposefully deleted and those that were deleted through various Windows-automated processes. This can also include temporary auto-save files, print.; spool files, deleted emails, and link files. The hexadecimal level also contains various items found in restore points and registry files that define hardware, such as external drives and websites visited, in addition to the document revisions and files created and maintained by the user.

The increased sophistication of Windows allows the computer system to store more information about how people use their computers. The forensic examiner will be able to uncover a large amount of data that relates to the use of a computer, what is or has been stored on it, and the

details about the user. In Microsoft's effort to "be all" to the user, it has incorporated ways to make computer use more secure, such as offering encryption and other methods to protect data from unwanted access. In the future, these types of innovations will stall the examiner arid will sometimes successfully prevent system access. However, these encryption packages are not always foolproof. The Encrypted File System offered by Microsoft has in fact been cracked bya number of password-cracking software makers.

Computer-forensic examiners have special tools and software designed to facilitate a thorough and legally sufficient analysis of items that contain digital evidence. It is important to allow a trained examiner to conduct a proper seizure and examination on a piece of evidence so the investigator will have the best chance of using that evidence in a legal proceeding. Whether an agency or company is defending against an unlawful termination suit or filing a criminal complaint, it is vital that the digital evidence is handled properly.

Handling the Evidence

One of the major differences between investigating computer-related crimes and conventional criminal activities is the volatility of the evidence that reside~ in the computers themselves. Indeed, the evidence of a computer intrusion might be erased or altered as part of the intrusion itself. It is therefore very important for the organisation and/or law enforcement personnel to deal quickly and decisively with evidence of suspected computer- related criminal activities.

Supported by a foundation for its introduction into court .Legally obtained .Properly identified .Properly preserved

In the handling of computer data in criminal investigations, the examiner *or* investigator must be aware of some of the vulnerabilities of computer evidence:

The investigator must ensure that turning off power to computer equipment will not destroy or erase evidence that is required for the investigation.

The read/write heads of hard disk drives must be parked in a retracted position so that powering down the disk drive will not cause the read/write head to contact the surface: of the disk platter.

Be aware that magnetic storage media are vulnerable to magnetic fields. Evidence might be erased without the investigator being aware of the erasure if the media are brought close to a magnetic field.

Be aware that other equipment attached to the computer might be: needed to complete the investigation into the data that resides in the computer.

The investigator should write-protect all disks that are being used in the investigation so that they cannot be written upon inadvertently.

Integrity of Evidence

There are certain issues that must be considered when processing computer evidence. These areas should be considered regardless of whether the incident will be processed criminally or civilly. Even if the organization decides not to take action, the way the investigation is

conducted can have potential civil-liability implications for both the organization and the fraud examiner.

Should the fraud examiner discover evidence on a computer system, he must be able to state unequivocally that the evidence was not changed in any way by his actions. This requires that

strict forensic methodologies be followed to satisfy the stringent evidentiary standards necessary to ensure the integ#ty o(the evidence "beyond a reasonable doubt" for possible court presentation. Th~refore, fraud examiners must be aware o£..the following issues that relate to the gathering of computer evidence.

Privacy Issues Regarding Computer Seizure Withoura Warrant

In every case where it becomes necessary to seize a computer or other device capable of storing digital evidence, the investigator should consult with legal counsel. It is imperative that legal counsel be involved in the seizure process and knowledgeable of case law pertaining to seizures in the workplace. Case law governing workplace seizures in the corporate community is different from case law governing seizures in the government workplace.

When conducting all internal investigation or inquiry into allegations of misconduct or illegal activities in both the private and governmental sector, it is important to be aware of what the employee policy protects against and what it allows. It should also be determined whether steps have been taken to nullify any expectations of privacy.

It should also be noted that personal devices are becoming more common in the workplace. Employees often carry PDAs, thumb drives, or MP3 players into the office. Each of these devices is capable of storing large amounts of data and can easily be used to steal a company's intellectual property.. Because these devices are often purchased by the employee for personal use, a search warrant may be needed to seize or search these devices because employees may

have a "reasonable expectation of privacy" in these types of personal devices. Therefore, it is extremely important to include such devices in the company's search policy.

Law Enforcement Assistance

There may be occasions when a fraud examiner will be called upon to assist law enforcement or to request the assistance of law enforcement in a particular case. Fraud examiners who are involved in law enforcement already understand the importance placed on proceeding with the search and seizure pursuant to a search warrant. Under these conditions, the law enforcement officer will prepare an affidavit for the search warrant, which will detail the probable cause or legal reasoning behind the request for the warrant. Only a judge can issue a search warrant and only law enforcement can seek and serve a search warrant. Often law enforcement personnel will need guidance from the fraud examiner as they conduct pre- search preparation.

Pre-Search Preparation

Obtaining as much intelligence as possible regarding the location of the potential evidence is very desirable before writing the search warrant affidavit. Considerations for fraud examiners include:

Determine the type of computer systems that will be involved in the search. What operating system is used? Are the computers networked together?

Determine how many people will be needed to conduct the search. In one case, approximately 17 networked file servers were involved, with multiple routers and dial-up modems. A team of only two investigators would need at least four to six hours to complete a seizure of this magnitude.

If expert witnesses with a specific expertise are required during the search, identify and clear them before the search warrant is written. Depending on the circumstances, their credentials should possibly be included in the warrant affidavit before they are approved by the magistrate issuing the search warrant~ The time to discover that an "expert witness" has a criminal conviction is before the search warrant affidavit has even been written, not when the witness takes the stand to testify in a criminal proceeding.

Search Warrant Affidavit Construction

Law enforcement personnel may seek the advice of the fraud examiner when constructing the search warrant affidavit. It is important to prepare an affidavit that includes all of the pertinent information, which will allow for a proper and legal search.

Question No 30. Checklist for Processing Electronically Stored Evidence for Removal.

The search for and seizure of technical equipment requires specific procedures that must be followed by fraud examiners to guarantee the integrity of evidence, and to protect both the organization and the individual fraud examiner from civil litigation. These guidelines are written to satisfy the evidentiary requirements for criminal prosecution, and each step in the process is there for a reason. Fraud examiners who deviate from these guidelines should be able to justify their actions if called into question later.

1. If possible, before executing a search warrant where computer equipment and/or magnetic storage media is to be seized, try to make sure that someone will be present who is familiar with computer equipment to assist in the identification of the various components.

2. It is critical that *anyone* not involved in the investigation be kept away from any computer equipment, and **not be allowed to touch any of the equipment!** This includes any person not directly involved in handling the computer and related equipment. It is possible for a suspect **or any person** touching only one key of a system keyboard (when a computer is operational) to destroy evidence. Limit the number of personnel responsible for processing computer-related evidence to maintain the integrity of this evidence.

3. If the person seizing the system has the appropriate training and expertise, it might be useful to observe the video display of the system. Information might be displayed that will be of value in the case. If this occurs, document with a close-up photograph of the video screen. (Take care if using a camera with a flash that the flash does not reflect back into the camera lens.)

4. If a computer or peripheral is not covered by the respective search warrant, leave it alone until a supplemental warrant can be obtained.

5. If the computer is to be removed from the location, do not enter anything via the system keyboard or attempt to read information from the system or any associated magnetic media.

6. Do not move the computer any more than is necessary until it is properly secured. Even then, extreme care should be taken, as sudden motion could cause the destruction of data or damage to the equipment itself.

7. Photograph the overall view of the computer system (wide view). Move the equipment as little as possible before taking this photograph to indicate how the equipment was originally positioned. Consider videotaping the confiscation procedure for complete documentation of all

actions performed. However, caution is advised, since the video will capture everything that is said and done. Speculative statements or levity should be restricted.

8. Document the state of the computer when first observed (was it operational, what was displayed on the monitor screen, etc.).

9. Depending on the experience of the person seizing the system, it might be advisable to unplug the power from the Central Processing Unit (CPU) before taking any further action. Unplug the power at the wall outlet, if accessible. Even though this action will lose any data in Random Access Memory, it might prevent the computer from deleting or changing other data. **NOTE: This applies to stand alone microcomputers only, and does not include computers connected to a Local Area Network (LAN).**

10. Turn off the power to all other components and/or pieces of peripheral equipment (such as printers, video display CRTs, or monitors, etc.). Be aware that many peripherals utilize Random Access Memory, which can contain evidence that will be lost when power is removed.

11. If possible, photograph all cable connections (usually in the rear of the system), before disconnecting.

12. Disconnect all components that are attached to an **external power supply only** (e.g., from an electrical wall socket, etc.).

13. Never connect or disconnect any of the cables of the system when the computer is operating. This could result in physical damage to the system components and/or peripheral equipment.

14. Label all cable connections, including any telephone cables that are connected to the system so that the system can be reconstructed at a later time for analysis.

15. Again, photograph all cable connections. Before photographing, try to arrange the cable connector labels in such a way that they will be visible in the photographs.

16. Label each item of equipment that will be confiscated. This includes the CPU, monitor, printers, etc. Each item that has a removable exterior case should be sealed with a tamperproof evidence tape (especially the CPU case). This will help to prevent later allegations that components were removed or altered.

17. Consideration should be given to separate close-up isolation photographs for each item to be seized. These close-up shots will serve the purpose of providing more specific identification of seized items, and responding to possible future allegations of physical damage to a seized item.

18. Document the location of all items seized (which room, specific location in the room, reference to photographs, the person who seized the item, serial numbers, special identification markings, etc.).

19. Check all floppy disk drives to determine if they contain a floppy disk. If so, remove the disk from the drive and place it in a disk sleeve. Write-protect the disk immediately. Label the particular disk drive to show which drive the disk came from, and then label a paper bag to indicate that the floppy disk was taken from the labeled drive. Place the disk in the paper bag and seal it.

20. Place a cardboard insert or a "throwaway" disk into the disk drive and secure the drive door shut to secure the drive heads for transportation. Cardboard inserts are specially made for this purpose. If none are available, a disk of the particular size that contains no data might be used (preferably a new, unused disk).

21. Check any other removable storage media drives, remove any storage media they contain, and label the media for identification purposes. (This includes components such as optical drives, external tape drives, IOMEGA drives, CD-Rom, etc.)

22. If there is any uncertainty as to what a piece of equipment is, do not speculate, just label the equipment with a unique identifying number and secure the item for later analysis. However, be prepared to justify the seizure of a component that might or might not be covered in the search warrant.

23. When all components and cables have been labeled and documented, disconnect the cables from their respective component and secure the cables.

24. If covered in the search warrant, confiscate all related manuals and other documentation, and all magnetic media. Also confiscate any other items that might be evidence in the case and that are covered by the terms of the search warrant.

25. If at all possible, after all equipment and magnetic media have been labeled and inventoried, each item should be stored in a paper bag or a cardboard box and sealed (to keep out dust). Large items, such as the CPU and/or printers could be stored in large paper bags or large boxes. Smaller items, such as floppy disks, could be stored in sandwich-bag sized paper bags. This practice will protect these items from unnecessary exposure to dust. An additional label should

be attached to the bag identifying the contents of the bag, along with any identifying numbers, such as the number of an evidence tag. **Note: Plastic bags (such as garbage and sandwich bags) should not be used to store evidence!**

26. Ensure that adequate support is given to all items when they are being moved.

27. Thoroughly document the inventory of everything to be removed from the location. This will be required for the search warrant return (if applicable), but also serves to provide a measure of liability protection for the person seizing the system.

Question No 31. What is Fraud Risk Assessment and Fraud Risk?

FRAUD RISK ASSESSMENT

There are many things that organizations can and should do to minimize the risk that fraud can occur and go undetected. A fraud risk assessment can be a powerful proactive tool in the fight against fraud for any business.

Regulators, professional standard-setters, and law enforcement authorities continue to emphasize the crucial role that fraud risk assessment plays in developing and maintaining effective fraud risk management programs and controls.

What Is Fraud Risk?

Cressey's Fraud Triangle teaches us that there are three interrelated elements that enable someone to commit fraud: the motive that drives a person to want to commit the fraud, the opportunity that enables him to commit the fraud, and the ability to rationalize the fraudulent behaviour. The vulnerability that an organisation has to those capable of overcoming all three elements of the fraud triangle is fraud risk. Fraud risk can come from sources both internal and external to the organisation.

Why Should an Organisation Be Concerned About Fraud Risk?

Every organisation is vulnerable to fraud; there is no organization that has immunity to that risk. The key to reducing that vulnerability is to be consciously aware and realistic about what the

organization's weaknesses are. Only then can management ensure that it can establish mechanisms that effectively prevent or detect fraudulent activities.

Organizational stakeholders expect thro stewards to be thoughtful and prudent about protecting the business. However, even when tales of fraudsters are getting a lot of public attention~ many organizations still have difficulty facing the realities of how susceptible they really are to fraud.

There are many factors that influence how at risk an organisation is to fraud. Some of the bigger factors are:

- The business it is in
- The environment in which it operates
- The effectiveness of the internal controls within the business processes .The ethics and values of the company and the people within it
- The Business It Is In

The types of risks an organisation faces are directly connected to the nature of business that it is engaged in. For example, the inherent fraud risks faced by hospitals and medical practices are vastly different from those faced by banks and financial institutions.

The Environment in Which It Operates

The environment in which the organisation operates has a direct impact on its vulnerability to fraud. Brick-and-mortar businesses have very different risk profllethan Internet businesses. Likewise, businesses in urban areas have different risk profiles businesses in rural areas. The environment in which the business operates can play a big role in influencing its vulnerability to fraud.

The Effectiveness of Internal Controls Within the Business Processes

A good systemofi1: lternal controls, with the right balance of preventive and detective controls, can greatly reduce an organization's vulnerability to fraud. Preventive controls are those manual or automated processes that stop something bad from happening before it occurs. Detective

controls can also be manual or automated, but are designed to identify something bad that has already occurred. No system of internal controls can fully eliminate the risk of fraud, but well-designed and effective internal controls can deter the average fraudster by reducing the opportunity to commit the fraud.

The Ethics and Values of the Company and the People within It

It is extremely difficult, if not impossible, to have a company made up of individuals whose ethics and values are fully aligned with those of the organisation. The gap in that alignment can significantly increase an organization's fraud risk.

Whilemanyorganis;!.tions have codes of conduct, those codes are not always very clear in drawing the definitive line between acceptable and unacceptable behaviour. That lack of clarity leaves a lot of wiggle room for fraudsters to rationalize their actions~ For example, in most organizations it is generally understood that manipulating financial records is unacceptable behaviour that will result in termination. However, it is not always apparent whether taking a pen or pencil home that belongs to the company is unacceptable behaviour or what the consequence, if any, would be.

An organisation that is clear and consistent about its ethics, values expectations for its people will reduce the potential fraudster's ability to rationalize his actions. Likewise, an organisation that demonstrates consistency and predictability in how it handles and holds accountable unacceptable behaviors can significantly reduce the risk of fraud;

What Is a Fraud Risk Assessment?

Fraud risk assessment is a process aimed at proactively identifying and addressing an organization's vulnerabilities to internal and external fraud. As every organisation is different, the fraud risk assessment process is often more an art than a science. Additionally, organizational fraud risks continually change. It is therefore important to think about a fraud risk assessment as an ongoing, continuous process, rather than just an activity.

A fraud risk assessment starts with an identification and prioritization of fraud risks that exist in the business.. The process evolves a~ the results of that identification and prioritization begin to

drive education, communication, organizational alignment, and action around effectively managing fraud risk and identifying new fraud risks as they emerge.

What Is the Objective of a Fraud Risk Assessment?

In the simplest terms, the objective of a fraud risk assessment is to help an organisation identify what makes it most vulnerable to fraud. Through a fraud risk assessment, the organisation is able to identify where fraud is most likely to occur, enabling proactive measures to be considered and implemented to reduce the chance that it could happen.

Why Should Organizations Conduct Fraud Risk Assessments?

Every organisation should conduct a fraud risk assessment and build procedures to keep the assessment process current and relevant. Not only is this practice good corporate governance, but it makes good business sense.

Improve Communication and Awareness About Fraud

Conducting a fraud risk assessment can be a great vehicle for an organisation. to open up communication and raise awareness about fraud. When employees are engaged in an open discussion about fraud, the conversations themselves can play a role in reducing fraud vulnerability. Employees are reminded that the organisation does care about preventing fraud and are empowered to come forward if they suspect fraud is occurring in the organisation. Open communication and awareness about fraud can also deter a potential fraudster by reducing his ability to rationalize bad behaviour and increasing his perception that someone might catch on to his actions and report him.

Identify What Activities Are the Most Vulnerable to Fraud

Management must know where the company is most vulnerable to fraud in order to prevent it from happening. For most companies, the normal. Course of business generally involves many different activities. However, riot all of the activities that the company engages in are equal in terms of increasing the business' exposure to fraud. The fraud risk assessment helps guide the organisation to focus on the activities that really put the company at greatest risk.

Know Who Puts the Organisation at the Greatest Risk

The actions of certain individuals can significantly increase the company's vulnerability to fraud. The risk can be driven from the way in which someone makes decisions, behaves, or treats others within and outside the organisation. The fraud risk assessment can help hone in on those people and their activities that may increase the company's overall fraud risk.

Develop Plans to Mitigate Fraud Risk

If management knows where the greatest fraud risks are, it can put plans in place to reduce or mitigate those risks. The fraud risk assessment provides a vehicle that can be used to ~ alignment amongst various stakeholders and drive action to decrease fraud risk.

Develop Techniques to Determine If Fraud Has Occurred in High-Risk Areas Assessing an area as a having high fraud risk does not conclusively mean that fraud is occurring there. However, the fraud risk assessment is useful in identifying areas to proactively investigate to determine whether fraud has in fact occurred.. In addition, putting activity in high-risk areas under increased scrutiny can deter potential fraudsters by increasing their perception of detection.

What Makes a Good Fraud Risk Assessment? A good fraud risk assessment is one that fits within the culture of the organisation, is sponsored and supported by the right people, encourages everyone to be open in his participation, and is generally embraced throughout the business as an important and valuable process. Conversely a fraud risk assessment that is conducted without these conditions will have inferior results.

The Right Sponsor

Having the right sponsor for a fraud risk assessment is extreme/important in ensuring its success and effectiveness. The sponsor must be senior enough in the organisation and command the respect of the employees to elicit full cooperation in the process. The sponsor has to be someone who is committed to learning the truth about where the company's fraud vulnerabilities really are. He can't be someone who is prone to rationalization or denial; he must be a truth seeker. In the ideal situation, the sponsor would be an independent board director or audit committee member. However, a good CEO or other internal senior leader can be equally as effective.

An organization's culture Plays a big part in influencing fraud vulnerability and risk. If the company's culture is shaped by a strong and domineering leader, it would be difficult to have that leader sponsor the fraud risk assessment and get candid, honest participation from the people in the business. Think about how effective a fraud risk assessment of Tyco International would have been with Dennis Kozlowski as its sponsor. Similarly, a fraud risk assessment of Enron would have been impossible with Kenneth Lay or Jeffrey Skilling as its sponsor.

The right sponsor is someone who is open and willing to hear the good, the bad, and the ugly. For example, let's say that the fraud risk assessment reveals that one of the greatest fraud risks facing the organisation is bribery/corruption based on the cozy nature of one of the key business leaders with the company's business partners. For the assessment to be fully effective, the sponsor needs to be independent and open in his evaluation of the situation and, most important, appropriate in his response to the situation.

Independence/Objectivity of the People Leading and Conducting the Work

A good fraud risk assessment can be effectively conducted either by people inside the organisation or with external resources. However, the people leading and conducting the fraud risk assessment need to be independent and objective throughout the assessment process. Additionally, they must also be perceived as independent and objective by others.

The people leading and conducting the work should be thoughtful and mindful about any personal biases they may have regarding the organisation, taking steps to reduce or eliminate all biases that may affect the fraud risk assessment process. For example, if an employee on the fraud risk assessment team had a very bad past experience with someone in the accounts payable department, he might allow that experience to affect his evaluation of the fraud risks related to that area of the business. To compensate for this bias, someone else should perform the fraud risk assessment work related to the accounts payable department's activities.

Cultural neutrality is an important aspect of independence and objectivity when leading or conducting a fraud risk assessment; Some organizations have very strong corporate cultures that can play a big role in influencing the way the people inside of the organisation think about fraud risk: If people within the organisation are leading and conducting the fraud risk assessment, they

must be able to step outside of the corporate culture to assess and evaluate the presence and significance of fraud risks in the business.

A Good Working Knowledge o/the Business

The individuals leading and conducting the fraud risk assessment need to have a good working knowledge of the business. Every organisation is unique; even companies that appear similar have characteristics that make them-and their fraud risks-different from their competitors. Some o(those differences can be obvious, while others are more subtle.

To ensure a good working knowledge of the business, the fraud risk assessor must know, at a more than superficial level, what the business does and how it operates. He must also have an understanding about what makes the organisation both similar to and different from other companies in related lines of business.

Obtaining information about broad industry fraud risks from external sources can be extremely helpful. Such sources include industry news; criminal, civil, and regulatory complaints and settlements; and professional organizations, such as the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners.

Access to People at All Levels of the Organisation

It is often said that perception is reality. In other words, how an individual perceives a situation is his reality of the situation. In an organisation, it is important to ensure that the perceptions of people at all levels get a voice in the fraud risk assessment process.

Leaders of a business or function often have very different perspectives from their subordinates about how something is perceived or executed. However, this does not always mean that one perspective is right and the other is wrong. What it does mean is that expectations and perceptions within the organisation are not aligned, which could increase fraud risk.

Engendered Trust

If the organisation and its employees do not trust the people leading and conducting the fraud risk assessment, they will not be open and honest about the realities of the business, its culture, and its vulnerability to fraud. Trust is hot something that can be granted by authority; it must be earned by words and actions.

The Ability to Think the Unthinkable

Most honest people are not naturally inclined to think like a fraudster. In fact, many large- scale frauds that have occurred would have been deemed unthinkable by people closest to the events. A good fraud risk assessment has to allow for the people leading and conducting the assessment to be expansive in their consideration and evaluation of fraud risk. Thoughts of "it can't happen here "should not be allowed to moderate the evaluation of fraud risk.

A Plan to Keep It Alive and Relevant

The fraud risk assessment should not be treated as a onetime exercise that is executed, reported on, and then put on a shelf to collect dust. The organisation should strive to keep the process alive and relevant through ongoing dialogue, active management of action plans, and development of procedures to ensure the assessments maintained on a content basis.

Considerations for Developing an Effective Fraud Risk Assessment

A fraud risk assessment is only effective if the organisation embraces it and uses the results to monitor, change; or influence the factors that put the company at risk for fraud.

Packaging It Right

People do not easily relate to or embrace things that they don't understand. Every organisation has its own vocabulary and preferred methods of communication (i.e., the language of the business). The notification and execution of the fraud risk assessment, including the reporting of the results, will only be effective if completed in the language of the business.

For example:

In a creative organisation where decisions are made based on qualitative assessments and instinct and where the majority of communication is visual, a quantitative approach to assessing fraud risk driven by numbers and calculations would most likely be rejected.

.In an organisation where the business is built and run on quantitative decision-making models, a qualitative approach with no quantitative components would most likely is rejected.

Therefore, the assessor must remain mindful of the language used throughout the fraud risk assessment. Specifically, he should stay away from technical language that won't resonate with people in the business. For example, many people in the business might not easily relate to or understand the term cash larceny. lf cash larceny is one of the organization's greatest fraud risks, it might be more effective to explain the concept in layman's terms and describe the risk as "theft of cash" instead.

One Size Does Not Fit All

Do not try to fit around peg into a square hole; what works in one organisation most likely will not easily work in another. Recognizing the nuances and differences of each business and tailoring the approach and execution to the specific organisation can help make the fraud risk assessment successful. While a generic framework or toolset can be a valuable starting point for the development of the fraud risk assessment, it must be adapted to fit the business model, culture, and language of the organisation.

Keeping It Simple

The more complicated the fraud the risk assessment is, the harder it will be to execute it and drive action. Whether the assessor uses a generic assessment framework or develops one specifically for the organisation, he should focus the effort and time on evaluating the areas that are most likely to have fraud risk.

Question No 32. How to prepare the Company for a Fraud Risk Assessment. How Fraud Risk Assessment should be conducted?

Preparing the company for the fraud risk assessment is a critical element to ensuring its success. The culture of the organisation should play a large role in influencing the approach taken to prepare the company for the fraud risk assessment. The goals of the preparation should be to:

- Assemble the right team to lead and conduct the fraud risk assessment.
- Determine the best techniques to use in conducting the fraud risk assessment.
- Obtain the sponsor's agreement on the work to be performed. .Educate the organisation and openly promote the process.

Assemble the Right Team to Lead and Conduct the Fraud Risk Assessment Before conducting the fraud risk assessment, the organisation should build a fraud risk assessment team consisting of individuals with diverse knowledge, skills, and perspectives that will lead and conduct the fraud risk assessment. The size of the team will depend on the size of the organisation and the methods used to conduct the assessment. The team members might include internal and external resources, such as:

- Accounting and finance personnel who are familiar with the financial reporting processes and internal controls
- Nonfinancial business unit and operations personnel who have knowledge of day- to-day operations, customer and vendor interactions, and issues within the industry
- Risk management personnel who can ensure that the fraud risk assessment process integrates with the organization’s enterprise risk management program
- The general counselor other members of the legal department
- Members of any ethics or compliance functions within the organisation .Internal auditors
- External consultants with fraud and risk expertise

- Any business leader with direct accountability for the effectiveness of the organization's fraud risk management efforts.

Determine the Best Techniques to Use to Conduct the Fraud Risk Assessment

There are many ways to go about conducting the' fraud risk assessment Picking a method or combination of methods that are culturally right for the organisation will help to ensure its success. The assessment team should also consider the best ways to gather rapid, truthful information from people throughout all levels of the organisation, starting by understanding what techniques are commonly and effectively used throughout the organisation.

Some examples of methods that can be used to conduct the fraud risk assessment are:

- Interviews
- Focus groups
- Surveys
- Anonymous feedback mechanisms

Interviews

Interviews can be an effective way to conduct a candid one-on-one conversation. The usefulness of interviews as a technique will depend on how willing people in the organisation are to be open and honest in a direct dialogue with the interviewer. The assessor must consider whether interviews are commonly and effectively used in the organisation to gather and elicit information. He should also speak with individuals that have previously conducted interviews with employees to glean lessons learned. For each potential interviewee, the assessor ~should gauge how likely and willing he would be to be open and honest some people may be good interview candidates, while others may need to be engaged through a different approach.

Focus Groups

Focus groups enable the assessor to observe the interactions of employees as they discuss a question or issue. Some topics may lend themselves to being discussed in an open forum in

which people feel comfortable among their colleague$. Additionally, when discussing tough or thorny issues in a group, an anonymous, real-time voting tool can be an effective way of opening up a dialogue amongst the participants.

The success of a focus group will be highly dependent on the skill of the facilitator. If focus groups are used as part of the fraud risk assessment, they should be) and by an experienced facilitator whom the group will relate to and trust. Getting a group to open up and talk honestly can be very difficult. An experienced facilitator will be able to read the group and use techniques, such as group icebreakers, to make the session a success.

Surveys

Surveys can be anonymous or directly attributable to individuals. Sometimes people will share more openly when they feel protected behind a computer or paper questionnaire. In an organisation where the culture is not one where people pinup and freely talk, an anonymous survey can be a great way to get feedback. However, employees can be skeptical about the true anonymity of a survey, especially-in organizations that use surveys to solicit feedback anonymously but send follow-up to individual delinquent respondents. If the assessor determines that an anonymous survey is an appropriate technique to use in the fraud risk assessment, he should clearly and explicitly explain to employees how anonymity will be maintained.

Anonymous Feedback Mechanisms

In some organizations, anonymous suggestion boxes or similar mechanisms are used to encourage and solicit frequent employee feedback. In these companies, information pertaining to the fraud risk assessment can be requested in the same way. Additionally, use of an anonymous feedback mechanism can also be effective in an environment where people are less likely to be open and honest through other methods and techniques. .

One approach to effectively using the anonymous feedback technique involves establishing a question of the day that is prominently displayed above a collection box. An example question is: "If you thought fraud was occurring in the company would you come forward? Why or why not?"

Another approach involves using a table lineup office to ten opaque boxes, each with a statement posted above it.. Employees are provided with poker chips in two different colors and told that one color indicates "I agree," and one indicates "I disagree.." Employees are then encouraged to respond to each statement by to putting a corresponding chip in each box to indicate their response.

Obtain the Sponsor's Agreement on the Work to be performed

Before the fraud risk assessment procedures begin, the sponsor and the fraud risk assessment team .need to agree on:

- .The scope of work that will be performed
- .The methods that will be used to conduct the work (e.g., surveys, interviews, focus groups, anonymous feedback mechanisms)
- .The individuals who will participate in the chosen methods .The content of the chosen methods
- .The form of output for the assessment

Educate the Organisation and Openly Promote the Process

The fraud risk assessment process should be visible and communicated throughout the business. Employees will be more inclined to participate in the process if they understand why it is being done and what the expected outcomes will be.

Sponsors should be strongly encouraged to openly promote the process. The more personalized the communication from the sponsor, the more effective it will be in encouraging employees to participate in the process. Whether it is a video, a town hall meeting, or e-mail, the communication should be aimed at eliminating any reluctance employees have about participating in the fraud risk assessment process.

Executing the Fraud Risk Assessment

The execution of the fraud risk assessment can be approached in many ways. The approach should be tailored to the organisation, but should be structured and rational to ensure its success. "

Choosing a Framework

When conducting a fraud risk assessment, it is helpful to use a framework for perfomiing, evaluating, and reporting on the results of the work. Fraud risk can be analyzed and reported both qualitatively and quantitatively using a consistent framework.

The following sample fraud risk assessment frameworks illustrate how the elements of fraud risk assessment are applied under different approaches.

Question No 33. Write down the Sample Fraud Risk Assessment Framework.

Using this framework; the fraud risk assessment team incorporates the following into the fraud risk assessment strategy:

1. Identify potential inherent fraud risks.

2. Assess the likelihood of occurrence of the identified fraud risks.

3. Assess the significance to the organisation of the fraud risks.

4. Evaluate which people and departments are most likely to commit fraud and identify the methods they are likely to use.

5. Identify and map existing preventive and detective controls to the relevant fraud risks.

6. Evaluate whether the identified controls are operating effectively and efficiently.

7. Identify and evaluate residual fraud risks resulting from ineffective or nonexistent controls.

The framework begins with a list of identified fraud risks, which are assessed for relative likelihood and significance of occurrence. Next, the risks are mapped to people and departments impacted and to relevant controls. Subsequently, the relevant controls are evaluated for design effectiveness and are tested to validate their operating effectiveness. Lastly, residual risks are identified, and a fraud risk response is developed to address them. The table below provides a visual representation of the steps involved in this framework, and can be filled in as the fraud risk assessment is performed.

Identify Potential** Inherent Fraud **Risks

The fraud risk assessment team should brainstorm to identify the fraud risks that could apply to the organisation. Brainstorming should include discussions regarding the following areas:

INCENTIVES, PRESSURES, AND OPPORTUNITIES TO COMMIT FRAUD

When assessing incentives, pressures, and opportunities to commit fraud, the fraud risk

Assessment team should evaluate:.

- Pressures on individuals to achieve performance or other targets and how such pressures may influence employees' behaviour
- Opportunities to commit fraud that arise from weak internal controls, such as a lack of segregation of duties

RISK OF MANAGEMENT'S OVERRIDE OF CONTROLS

When considering the potential for management's override of controls, the fraud risk assessment team should keep in mind that:

- .Management personnel within the organization generally know the controls and standard operating procedures that are in place to prevent fraud.
- .Individuals who are intent on committing fraud may use their knowledge of the organization’s controls to do it in a manner that will conceal their actions.

FRAUDULENT FINANCIAL REPORTING

Potential fraudulent financial reporting risks include:

- .Inappropriately reported revenues, expenses, or both
- .Inappropriately reflected balance sheet amounts, including reserves
- .Inappropriately improved or masked disclosures .Concealed misappropriation of assets

- .Concealed unauthorized receipts, expenditures, or both
- .Concealed unauthorized acquisition, disposition, or use of assets

ASSET MISAPPROPRIATIONS

Potential asset misappropriation risks include misappropriation of: .Tangible assets

.Intangible assets

.Proprietary business opportunities

CORRUPTION

Potential corruption risks include:

- .Parent of bribes or gratuities to companies, private individuals, or public officials .Receipt of bribes, kickbacks, or gratuities
- .Aiding and abetting of fraud by outside parties, such as customers or vendors
- Certain other types of risks that can affect or be affected by each of the major ateas of fraud risks include regulatory and legal misconduct, reputation risk, and risk to information technology (11).

REPUTATION RISK

The fraud risk assessment team should ensure that consideration of reputation risk is part of the organization's risk assessment process because fraudulent acts can damage an organization's reputation with customers, suppliers, capital markets, and others.

RISK TO INFORMATION TECHNOLOGY

Information technology (J'ry is a critical component of fraud risk assessment. Organizations rely on IT to conduct business, communicate, and process financial information. A poorly designed or inadequately controlled IT environment can exposé an organisation to threats to data integrity, threats from hackers to system security, and theft of financial and sensitive business information. Whether in the form of hacking, economic espionage, Web defacement, sabotage of data, viruses, or unauthorized access to data, IT fraud risks can result in significant financial and information losses.

Assess the Likelihood reoccurrence of the Identified Fraud Risks

Assessing the likelihood and significance of each potential fraud risk is a subjective process that allows the organisation to manage its fraud risks and apply preventive and detective controls rationally. The fraud risk assessment team should first consider fraud risks to the organisation on an inherent basis, or

without consideration of known controls. By approaching the assessment in this manner, the team will be better able to consider all relevant fraud risks and the? Evaluate and design controls to address the risks.

The likelihood of occurrence of each fraud risk can be classified as *remote, reasonably possible,* or *probable.* The fraud risk assessment team should consider the following factors in assessing the likelihood of occurrence of each fraud risk:

Question No 34. How organization should respond to different risks.

Response to Fraud Risks:

Regardless of the framework used to conduct the fraud risk assessment, management will need to address to the identified risks. Larry Cook, CFE, who is the principal author of the ACFE Fraud Risk Assessment Tool, suggests that management can use one or a combination of the following approaches to respond to the organization's residual fraud risks:

Avoid the Risk

Management may decide to avoid the risk by eliminating an asset or exiting an activity [the control measures required to protect the organisation against an identified threat are too expensive. This approach requires the fraud risk assessment team to complete a cost-benefit analysis of the value of the asset or activity to the organisation compared to the cost of implementing measures to protect the asset or activity.

Transfer the Risk

Management may transfer some *or* all *of* the risk by purchasing fidelity insurance or a bond. The cost to the organizations the premium paid for the insurance or bond. The covered risk of loss is then transferred to the insurance company, less any deductible payment included in the contract.

Mitigate the Risk

Management can help mitigate the risk by implementing appropriate countermeasures, such as prevention and detection controls. The fraud risk assessment team should evaluate each

countermeasure to detertnine if it is cost effective andreasonib1e given the probability of occurrence and impact Qf.1oss.

Assume the Risk

Management may choose to assume the risk if it determines that the probability of occurrence and impact of loss are low. Management may decide that it is more cost effective to assume the risk than it is to eliminate the asset or exit the activity, buy instance to transfer the risk, or implement countermeasures to mitigate the risk.

Combination Approach

Management may also elect a combination of the above approaches. For example, if the probability of occurrence and impact of loss are high, management may decide to transfer part of the risk through the purchase *of* insurance, as well as implement preventive and detective contro1s to mitigate the risk.

Question No 35. ERM is considered now a day's vital framework for managing risk. Agree or not.

ENTERPRISE RISK MANAGEMENT (ERM)

What is Enterprise-wide Risk Management?

People undertake risk management activities to identify, assess, manage, and control all kinds of events or situations. These can range from single projects or narrowly defined types of risk, e.g. market risk, to the threats and opportunities facing the organization as a whole. The principles presented in this paper can be used to guide the involvement of internal auditing in all forms of risk management but we are particularly interested in enterprise-wide risk management because this is likely to improve an organization's governance processes.

Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Responsibility for ERM

The board has overall responsibility for ensuring that risks are managed. In practice, the board will delegate the operation of the risk management framework to the management team, who will be responsible for completing the activities below. There may be a separate function that co-ordinates and project-manages these activities and brings to bear specialist skills and knowledge.

Everyone in the organization plays a role in ensuring successful enterprise-wide risk management but the primary responsibility for identifying risks and managing them lies with management.

Benefits of ERM

ERM can make a major contribution towards helping an organization manage the risks to achieving its objectives. The benefits include:

- ✓ Greater likelihood of achieving those objectives;
- ✓ Consolidated reporting of disparate risks at board level;
- ✓ Improved understanding of the key risks and their wider implications;
- ✓ Identification and sharing of cross business risks;
- ✓ Greater management focus on the issues that really matter;
- ✓ Fewer surprises or crises;
- ✓ More focus internally on doing the right things in the right way;
- ✓ Increased likelihood of change initiatives being achieved;
- ✓ Capability to take on greater risk for greater reward and
- ✓ More informed risk-taking and decision-making.

The activities included in ERM

- ✓ Articulating and communicating the objectives of the organization;

- ✓ Determining the risk appetite of the organization;
- ✓ Establishing an appropriate internal environment, including a risk management framework;
- ✓ Identifying potential threats to the achievement of the objectives;
- ✓ Assessing the risk (i.e. the impact and likelihood of the threat occurring);
- ✓ Selecting and implementing responses to the risks;
- ✓ Undertaking control and other response activities;
- ✓ Communicating information on risks in a consistent manner at all levels in the organization;
- ✓ Centrally monitoring and coordinating the risk management processes and the outcomes, and
- ✓ Providing assurance on the effectiveness with which risks are managed.

Providing assurance on ERM

One of the key requirements of the board or its equivalent is to gain assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level.

It is likely that assurance will come from different sources. Of these, assurance from management is fundamental. This should be complemented by the provision of objective assurance, for which the internal audit activity is a key source. Other sources include external auditors and independent specialist reviews. Internal auditors will normally provide assurances on three areas:

Risk management processes, both their design and how well they are working;

Management of those risks classified as ‘key’, including the effectiveness of the controls and other responses to them; and Reliable and appropriate assessment of risks and reporting of risk and control status.

Disbursement and Accounts Payable Fraud Schemes

The ultimate objective of any disbursement scheme is a check issued by the organization which is then converted to cash for personal gain. Managers often think that the check issuance process is unimportant. After all, it's just paper.

In state agencies in Washington, this type of fraud accounts for 85% of all losses over the past decade. It's too big to ignore, and very easy to defend against. The prime suspect is the bookkeeper.

The most common disbursement fraud involves a bookkeeper who issues checks to themselves or to others (i.e.; family and false vendors). Looking at the redeemed checks is the primary defense against this fraud. Knowing who you do business with is the primary defense in identifying checks issued to false vendors.

The Subtle Compromise of the Accounts Payable System

Managers and auditors should always look for a straight line from transaction initiator to accounts payable to check distribution process in the accounts payable system. This same principle also applies in the payroll system except that the straight line is from the source (the individual) to the approval point (the supervisor) and then to the payroll function for payment.

These transactions may not receive the same level of care in the authorization and approval process. The governing body may not have even approved these transactions.

Storage and issue controls over checks must be appropriately maintained. Blank (unnumbered) checks are high risk and require an even greater level of security than pre numbered checks.

Negotiable instruments (i.e.; checks) are being stolen and redeemed without the authorization and approval of the organization. Use locked storage facilities and limit the number of employees who have access. Monitor the inventory of negotiable instrument stocks. Maintain logs for negotiable instruments issued. Promptly note sequence breaks from one run to the next.

Act promptly with a "stop payment action" when numbers are missing. Determine whether an investigation is needed or if a police report should be filed.

At the heart of every fraud is a **missing or fraudulent** (falsified or altered) document. Don't use the **FIDO** concept (i.e.; "forget it, drive on". If you can't find the document supporting the transaction, your test fails. Find the right answer instead. The document may just be out of file for some legitimate purpose or reason.

Most disbursement frauds employ **common and simple methods**. Engage the mind and use your experience. Common sense is your most valuable resource. Since normal expenditures are repetitive in nature, scan the check register for suspicious transactions by concentrating on variances from the norm. Review disbursements for fictitious vendors, duplicate payments, overpaid employees, and payments to "cash" or financial institutions. For false vendors, compare like data elements from the personnel/payroll system to vendor files. Review invoices for generic office supply documents, pre numbering (make sure you don't get all the numbers, as in the only customer), post office box addresses only, lack of telephone numbers, etc. Compare the amount, payee, and endorsement on redeemed checks to the actual check register for a specified period of time (block sample). Multiple endorsements are high risk documents.

The **accounting entry for disbursement fraud** is debit expense, assets, revenue, liabilities or fund balance and credit cash.

Since disbursements fraud is recorded in the accounting system, and since the attributes of concern are "**what's too high or what's too much**". Disbursement fraud is concealed in accounts with **high volumes** of activity and/or **high dollar** amounts. Awareness of these fraud indicators is the key to fraud detection, and detection is everyone's job. Therefore, a comparative analysis of expenditures should look for these key elements within each organization.

Fraud perpetrators are unpredictable as to position and background. They change over time with the internal control system – **the "chameleon" effect**. It's difficult to distinguish original documents from **false original** documents. The critical element is whether or not the service was actually received.

The accounts payable function should never pay an invoice that has not been authorized and approved by the recipient of the goods and services. There are some companies that exist solely

or the purpose of sending **fictitious billings** to unsuspecting organizations, simply hoping the organization will pay the bill without researching the transaction.

Pay from **original source documents** only. Do not pay from Xerox copies of documents. While facsimile documents are "original" documents under the law, and are often needed to make urgent payments, always require the vendor to mail you a copy of the original document. The original document should then be filed with the supporting documents for the expenditure.

Question vendor invoices that **do not have a street address** (i.e.; post office box address only) or a vendor who is **not listed in the telephone book**.

Make sure that all supporting **documents are valid** and represent actual purchases of goods and services. Watch out for "**cut-and-paste**" documents where all the detail is missing from the transaction. If an employee has to write the description of the item purchased on the receipt, it's a high risk transaction. Determine if the receipt submitted for reimbursement purposes is the actual receipt type issued by the vendor involved. Confirm validity if necessary. And, never accept a receipt without appropriate vendor information recorded on the document. Watch for **numerical sequencing** of receipts or invoices used for reimbursement purposes.

Identify documents that serve the same purpose as **blank checks**, such as petty cash documents, travel vouchers, and time cards. Look for **a straight line** from source to approval to payment.

Eliminate the use of blank lines on these forms by crossing them out after the last item for approval. All fraud is after approval by a manager.

Don't accept the first plausible explanation for exceptions found, and make sure that an **independent party** analyzes and researches all complaints (customer feedback). The first defense is things are a mess here (by design when fraud occurs), it's an accounting problem (whatever that means), it's miscoded, or you simply just don't understand (the problem is that you do). Test all answers received. Be from Missouri, the "show me" state. Show me a transaction which when processed correctly will create this condition. There are none for fraudulent transactions.

Computer frauds are no different than manual frauds. Sometimes the only difference is that the records are maintained on computer storage media (i.e.; disks, drums, etc.) rather than in filing cabinets.

Checking Accounts and Imprest Funds – The Check Fraud Risk – Bogus Checks

The number one fraud in the United States, and probably the rest of the world for that matter, is the huge risk that exists today for a fraud scheme that involves the issuance of "bogus" checks by individuals outside the government. So, what can be done about this menace.

It's important for all public organizations to understand the risk posed by bogus checks. Check fraud in the United States is a $20 billion industry that is growing at the rate of about $1 billion presented to their bank for payment almost every business day.

Producing bogus checks is a rather simple and unsophisticated process. Anyone with a few thousand dollars in computer and peripheral equipment can produce high-quality bogus documents. And it doesn't take more than a day to recover this initial investment. The perpetrators only need your bank account number, and this information is provided on every check issued. Bogus electronic debit transactions can also be created.

Banks have accepted responsibility for most of the losses resulting from these fraud schemes because public organizations have promptly detected the bogus checks during the independent party bank reconciliation process. In some cases, banks have detected the counterfeit checks when presented for payment.

In response to this risk, many public organizations have established either "positive pay" or "reverse positive pay" at their banks. This is a daily reconciliation of the checks issued versus the negotiable instruments being presented for payment. While both of these systems work, positive pay is the preferred method of choice, even though it is the more expensive of the two options. An organization may also accomplish this reconciliation by using its on-line banking capability.

• **Positive pay**. This is an automated service provided by banks to detect bogus checks. It is extremely effective when the organization sends specific information to the bank on days when checks are issued. The bank compares the documents that come in by number and amount to a file of documents issued by the organization. If the bank has no in-file match, it contacts the organization to determine the negotiable instrument's authenticity. Two days are usually allowed for this process, but the process works better if the review is performed immediately. Counterfeit checks are then returned unpaid.

• **Reverse positive pay**. This method allows the organization to conduct its own daily matching procedures. Most banks offer customers a daily transmission of paid items that can be compared

with the organization's issued check file. The organization must promptly research each suspicious document and advise the bank of items to be returned.

If a public organization checking account becomes the target of a fraud scheme in the private sector, the Fraud Department at Equifax, a check guarantee company, can also put a hold on the account. The company can be reached at 1-800-337-5689. The local law enforcement agency should also be contacted. Closing the bank account is another option.

The State Auditor's Office takes this issue very seriously and wants to make sure that all public organizations understand the risk from bogus checks. For example, two cases have been reported where legitimate vendors created checks for an employee purchase and a delinquent loan payment.

Travel Vouchers

Travel vouchers can be high-risk transactions because of the possibility of employee manipulations. Fraudulent transactions are usually processed by one employee and are not a systemic problem for the organization. Since Department managers and other supervisors routinely review the travel vouchers for staff members, the highest risk employees who would be able to prepare and process a fraudulent travel vouchers are key managers, department heads, elected public officials, and employees in the accounts payable function. Therefore, concentrate periodic review efforts on higher levels of management officials. Concepts that can help:

The **state per diem system** is preferred over an **"actual" expense system**. Actual expenses are more costly to review and audit, with no significant improvement in the quality of supporting documents. There are many opportunities for fictitious supporting documents to be prepared and submitted for review and approval. Sequential receipts are submitted for expenses at various obtain reimbursement for items that are not otherwise authorized. Employees incur unauthorized expenses or purchase gifts and alcoholic beverages in violation of organization policies.

Inappropriate supporting documents are filed with the travel voucher. These include copies of documents rather than originals, charge slips rather than actual receipts, etc. Credit card statements are not a receipt. It's the underlying transaction receipt that is important.

Obtain them. Do not pay from statements only.

Meals and lodging provided by others while attending conferences must be excluded/deducted from employee reimbursement requests. A copy of the conference documents should be standard support for any such travel voucher.

Direct billings by hotels and others must be compared to employee travel vouchers to ensure duplicate expenses are not claimed.

Employee travel expenses for more than one organization should be filed on a single travel voucher and provided to each applicable organization. Original receipts should be filed with the host organization. If there is any question about documentation for such travel, contact the other organization to verify that each organization is paying the correct expenses for the travel. When employees file false travel vouchers for this travel, original source documents are filed with one organization while copies of these documents are filed with the second organization to obtain duplicate reimbursement for the same expenses.

Mileage for employee vicinity travel should be reasonable. Falsifications are difficult to detect.

But, obvious errors can be detected by comparing the individual's time sheet to the travel voucher, and by comparing the individual's vicinity travel voucher to travel vouchers for other specific events during the same time period. These reviews are often not accomplished because of the timing differences in receipt of these documents by managers and supervisors.

Periodically review all documents together for specific high risk employees. Duplications or other irregularities occur, such as vicinity travel while out of town on other official business, vicinity travel while not on duty, and vicinity travel when the employee's telephone records indicate a presence in the individual's primary office (i.e.; travel not likely or probable). Determining the individual's physical "imprint" at the office is critical to understanding what really occurred.

Purchasing

Collusion between a vendor and an organization employee is very difficult to detect, primarily because the employees openly circumvent the system of internal control.

Since off-book purchasing frauds are found as a result of tips and complaints, the organization must have an internal and external communication process that restricts access to buyers by using a central vendor reception area, and informs vendors of organization policies regarding gifts to employees and conflicts of interest. Determine whether the organization sends letters

(initial letter and reminder "holiday" letter) to vendors about its **policy on gifts and other inappropriate acts** between its employees and vendors.

Determine if assets are picked-up directly from vendors or delivered to non-standard delivery destinations, versus delivery to a **central delivery destination**. Exceptions to normal procedures should be reviewed very carefully.

Determine if assets are signed-for as received by an organization employee and signed-for as authorized for payment by an organization employee, the two primary signatures noted on purchasing documents. However, also determine if **the positions of the individuals** involved.

Employees **act out of character** by doing something that is not a part of their normal job description when fraud is involved.

Determine if vendor invoices include the narrative **description of the items purchased**, particularly on parts for vehicle and maintenance activities. These documents should not include only the part number for the item received. If so, request the vendor to provide the description of the item on future billings. If you can't get them, find another vendor who will provide this important information. The bottom line question is: "**What are you buying?**"

For credit card purchases, ensure that the original source documents support each line item listed on the monthly statement. Do not pay directly from statements without this support. All credit card fraud involves employees making **personal purchases** for their own use. Abuses have occurred for gasoline credit cards and all other types of purchasing credit cards.

Know Forms of Fraud

There are as many ways to cheat on an expense account as there are employees willing to cheat, but four common methods are:

1. Mischaracterizing expenses. This involves legitimate receipts for nonbusiness-related activities. If Joe treats his buddy John to a birthday dinner, for example, that generates an actual receipt, but it shouldn't show up on Joe's expense account.

2. Requesting multiple reimbursements. This is a riskier scheme, but just as simple. If Joe wants you to pay for John's birthday dinner twice, he can just copy the receipt and turn it in on

another expense report. Worse, he can attempt to be paid once for the bill, once for the receipt and once for the credit card statement.

3. Overstating expenses. When people overstate expenses, they request reimbursement for more than they spend. Changing a 3 to an 8 or a 1 to a 4 on a receipt is one popular approach.

4. Inventing Expenses. This is probably the easiest way for an employee to get you to foot more than your share of the bill. All Jane needs to do is ask a cabbie for an extra receipt, fill it out with the numbers of her choice and turn it in for reimbursement.

These and other small expense account infractions can add up to outrageous sums. In one case, a senior vice president who traveled extensively for business was found to have defrauded his firm of $30,000 over the course of three years by adopting a liberal definition of allowable business expenses.

PAYROLL FRAUD

Fraud through the payroll department is commonly committed by using ghost employees, inflating hours of work and overtime, as well as overstating expense accounts or medical claims.

Case Study: Simple Payroll Fraud

The bookkeeper of a construction company knew there were hundreds of transient workers on the payroll at any given time. She also knew that at any point in time, many workers dropped off the payroll and many more joined. She also knew that no one was checking her work. She handled the payroll, used the owner's facsimile signature stamp on checks, and hand-delivered the checks to the various jobsites!

The bookkeeper kept a handful of former employees on the payroll, bothmale and female. She even paid their union dues and payroll taxes! However, instead of delivering these checks to the jobsite, where of course the employees no longer worked, she endorsed the back of the checks and deposited them into her bank account. She was friendly with one particular teller at the bank branch and used this teller exclusively to deposit the checks. Several people at her employer were curious as to her new executive automobile, new home, and rumored house at the beach, which she passed off as the result of her husband's large win at the casino.

However, it took an enforced prolonged illness and absence from the office for a temporary bookkeeper to question why non-employees were still on the payroll. Ultimately, the company recovered just about all of its lost funds, including refunds from the union and the IRS together with recoveries from the bank and the fraudulent bookkeeper.

Case Study: Expense Report Fraud

For some reason, expense accounts have been the most overlooked and least controlled area of many companies. Some supervisors give these reports a cursory review and if they pass the "smell test," they are authorized.

Imagine the horror of a company that discovered that a particular employee's "authorized" expense reports had not in fact been authorized. She had forged the signatures of her supervisors and hand-delivered her expense reports to the accounting department, each time concocting an excuse why they did not come through the customary route of other employees' expense reports.

The embezzler was later described as a "smooth talker" who distracted others with her line of conversation. Over the course of four years, she submitted expense reports with several hundred thousand dollars of falsified expenses. She even went as far as creating false invoices submitted with her expense reports as support for her expenses. She included vouchers for business publication subscriptions, where she would show her credit card as having been used to incur the original expense, when in fact she hadn't even submitted the application for the subscription.

As is typical in many of these situations, her scheme was never found out while she was in the company's employment. She actually was dismissed for a totally unrelated insubordination issue. In the interim, she had become bold and mailed an invoice to the company from a fictitious vendor using a post office box, which did not reach the bookkeeping department until after she had been dismissed. A keen and skeptical clerk ran some Internet searches and internal reports and discovered the post office box had actually been used by the now former employee. After further investigation, her entire scheme was discovered.

The company recovered much of its loss from its insurance carrier and the perpetrator was sentenced to time in prison.

FRAUDULENT BILLING SCHEMES

These frauds are usually committed by outsiders such as vendors, suppliers, and contractors of various kinds. They are perpetrated through submission of false invoices for goods or services

not supplied or inflated invoices for goods or services of inferior quality. These frauds often involve collusion between outsiders and internal employees and can become quite complex. Collusion allows controls to be circumvented.

Case Study: Construction Fraud

Because the competitive bidding process for construction contracts often makes profit margins razor thin, contractors may be tempted to increase their profits through fraud. A developer negotiated a $550 million guaranteed maximum price contract with a prime contractor and subcontractors to erect a 40-story building. To the developer's surprise, the allowances and contingency holds for unexpected costs and emergencies were exhausted before even the core and shell had been completed. This left the interior work unfunded. Puzzled and suspicious, the developer hired private investigators who discovered the prime contractor had bribed the architect and they were now colluding to defraud the developer. The contractor was purchasing goods and services beyond those required for the developer's building, diverting the excess to other jobs on which he and the architect were working and submitting the invoices to the developer.

The excess expenses were approved and explained away by the architect. The contractor and the architect had convinced themselves that the developer's cost controls were shortsighted and would make the job unprofitable for them.

When the architect and contractor were confronted with the evidence of the private investigation, they agreed to pay for the remaining construction from their own funds rather than be prosecuted.

The developer did not press charges against either the architect or the contractor, but he did report the architect to the licensing board. At the hearing, the investigators produced the evidence they had discovered for the developer and the architect received a written reprimand. This effectively put the architect on an industry blacklist, which made it difficult for him to find well-paying jobs. As with other fraudsters, the consequences of the dishonest architect's fraud affected his family. He was no longer able to keep his children in private school, and he had to drop a club membership he had enjoyed with his wife. Life went on, but not at the carefree level the family had enjoyed before.

Bribery

Generally, bribery and corruption are off-book frauds that occur in the form of kickbacks, gifts, or gratuities to government employees from contractors or to private business employees from vendors.

At its heart, a bribe is a business transaction, albeit an illegal or unethical one. A person "buys" something with the bribes he pays. What he buys is the influence of the recipient. Bribery schemes can be difficult and expensive. Though they are not nearly as common as other forms of occupational fraud such as asset misappropriations, bribery schemes tend to be much more custody.

There are two basic reasons why a bribe occurs:

- ✓ .Because the transaction is not in the interests of the organisation for whom the person being bribed acts. Therefore, if the other party wants the transaction to be effected, it is necessary to bribe that person.
- ✓ .Although the person receiving the bribe may be acting in the best interests of his organisation by agreeing/approving the transaction, he may refuse to act until he has received the bribe. This may be the convention of the industry/country in which he is operating and accepted by the person offering the bribe not as immoral but as a necessary expense and in the interests of his own organisation.

Bribery is often defined as the offering, giving; receiving, or soliciting anything of value to influence an official act. The term official act means that bribery only encompasses payments made to influence the decisions of government agents or employees.

Many occupational fraud schemes, however, involve commercial bribery, which is similar to the traditional definition of bribery except that something of value is offered to influence a business decision rather than an official act of government. Commercial bribery may or may not be a criminal offense. For example, in the United States there is no general federal law prohibiting

commercial bribery all instances. However, there are statutes prohibiting bribery of employees of financial institutions to influence a loan. Therefore, the law of your particular jurisdiction and the facts of the case will determine whether bribery in the private sector may be prosecuted criminally. Commercial bribery can often be pursued in the civil courts as breach of fiduciary duty or conflict of interest.

Bribery schemes generally fall into two broad categories: kickbacks and bid-rigging schemes. Kickbacks are undisclosed presents made by vendors to employees of purchasing companies. The purpose of a kickback is usually to enlist the corrupt employee in an overbilling scheme. Sometimes vendors pay kickbacks simply to get extra business from the purchasing company. Bid-rigging schemes occur when an employee fraudulently assists a vendor in winning a contract through the competitive bidding process.

Kickback Schemes

Kickbacks, in the commercial sense, receiving anything of value to influence a business decision without the employer's knowledge and consent. Kickback schemes are usually very similar to the billing schemes described in the Asset Misappropriation section. They involve the submission of invoices for goods and services that are either overpriced or completely fictitious.

Kickbacks are classified as corruption schemes rather than asset misappropriations because they involve collusion between employees and vendors. In a common type of kickback scheme, a vendor submits a fraudulent or inflated invoice to the victim organisation and an employee of that organisation helps make sure that a present is made on the false invoice. For his assistance, the employee-fraudster receives a payment from the vendor. This present is the kickback.

Kickback schemes almost always attack the purchasing function of the victim company, so it stands to reason that these frauds are often undertaken by employees with purchasing responsibilities. Purchasing employees often have direct contact with vendors and there tore have an opportunity to establish a collusive relationship.

Diverting Business to Vendors

In some instances, an employee-fraudster receives a kickback simply for directing excess business to a vendor. There might be no overbilling involved in these cases; the vendor simply pays the kickbacks to ensure a steady stream of business from the purchasing company.

If no overbilling is involved in a kickback scheme, one might wonder where the harm lies. Assuming the vendor simply wants to get the buyer's business and does not increase his prices or bill for undelivered goods and services, how is the buyer harmed? The problem is that, having bought off an employee of the purchasing company, a vendor is no longer subject to the normal economic pressures of the marketplace. This vendor does not have to compete with other suppliers for the purchasing company's business, and so has no incentive to provide a low price or quality merchandise. In these circumstances the purchasing company almost always ends up overpaying for goods or services.

EXAMPLE

A travel agent ;)' provided free travel and entertainment to the purchasing agent Of a retail company. In return, the purchasing agent agreed to book all corporate trips through the travel agent. The victim company estimated that it paid 110,000 more for airfare over a two-year period by booking through the come/pt travel agent;)' than if it had used a different company.

Once a vendor knows it has an exclusive purchasing arrangement, its incentive is to raise prices to cover the cost of the kickback. Most bribery schemes end up as overbilling

Schemes even if they do not start that way. This is one reason why most business codes of ethics prohibit employees from accepting undisclosed gifts from vendors. In the long run, the employee's company is sure to pay for his unethical conduct.

Overbilling Schemes

EMPLOYEES WITH APPROVAL AUTHORITY

In most instances, kickback schemes because overbilling schemes in which a vendor submits inflated invoices to the victim organisation. The false invoices either overstate the cost of actual

goods and services, or reflect fictitious sales. The vendor in a kickback scheme generally seeks to enlist the help of an employee with the authority to approve payment of the fraudulent invoices. This authority ensures payment of the false billings without undue hassles.

EXAMPLE A manager was authorized to purchase fixed assets for his company as part of a leasehold improvement. The materials he ordered were of a cheaper quality and lower price than what was specified, but the contract he negotiated did not reflect this. Therefore, the victim company paid for high-quality materials, but received low-quality materials. The difference in price between .the time cost of the low-quality materials and what the company paid was diverted back to the manager as a kickback.

The ability of the employee to authorize purchases (and thus to authorize fraudulent purchases) is usually a key to kickback schemes. If the fraudster can authorize payments himself, he does not have to submit purchase requisitions to an honest superior who might question the validity of the transaction.

FRAUDSTERS LACKING APPROVAL AUTHORITY

While the majority of kickback schemes involve persons with authoritY to approve purchases, this authority is riot an absolute necessity. When an employee cannot approve fraudulent purchases himself, he can still orchestrate a kickback scheme if he can circumvent accounts payable controls. In some cases, all that is required is the filing of a false purchase requisition. If a trusted employee tells his superior that the company needs certain materials or services, this is sometimes sufficient to get a false invoice approved for payment. Such schemes are generally successful when the person with approval authority is inattentive or when he is forced to rely on his subordinate's ~dance in purchasing matters.

Corrupt employees might also prepare false vouchers to make it appear that fraudulent invoices are legitimate. Where proper Controls are in place, a completed voucher is required before accounts payable will pay an invoice. One key is for the fraudster to create a purchase order that corresponds to the vendor's fraudulent invoice. The fraudster might forge the signature of an authorized party on the purchase order to show that the acquisition has been approved. Where the

payables system is computerized, an employee with access to a restricted password can enter the system and authorize payments on fraudulent invoices.

In less sophisticated schemes, a corrupt employee might simply take a fraudulent invoice from a vendor and slip it into a stack of prepared invoices before they are input into the accounts payable system. A more detailed description of how false invoices are processed can be found in the Billing Schemes section.

Kickback schemes can be very difficult to detect.. In a sense, the victim company is being attacked from two directions. Externally, a corrupt vendor submits false invoices that induce the victim organisation to unknowingly pay for goods or services that it does not receive. Internally, one or more of the victim company's employees waits to corroborate the false information provided by the vendor.

Other Kickback Schemes

Bribes are not always paid to employees to process phony invoices. Some outsiders seek other fraudulent assistance from employees of the victim organisation. For ins~nce, inspectors are sometimes paid off to accept substandard materials, or to accept short shipments of goods.

Representatives of companies wishing to purchase goods or services from the victim organisation at unauthorized discounts sometimes bribe employees with billing authority. The corrupt employees make sales to their accomplices at greatly reduced rates---sometimes even selling items at a loss--and in return they receive a portion of the discount.

Kickback Payments

It should also be noted that every bribe is a two-sided transaction. In every case where a vendor bribes a purchaser, there is someone on the vendor's side of the transaction who is making an illicit payment. It is therefore just as likely that your employees are paying bribes as accepting them.

In order to obtain the funds to make these payments, employees usually divert company money into a slush fund, a non company account from which bribes can be made. Assuming that bribes are not authorized by the briber's company, he must find away to generate the funds necessary to

illegal influence someone in another organisation. Therefore, the key to the crime from the briber's perspective is the diversion of money into the slush fund. This is a fraudulent disbursement of company funds, which is usually accomplished by the writing of company checks to a fictitious entity or the submitting of false invoices in the name of a false entity. Payments to a slush fund are typically coded as "fees" for consulting or other services;

It is common to charge fraudulent disbursement$ to nebulous accounts like "consulting fees." The purchase of goods can be verified by a check of inventory, but there is no inventory for these kinds of services. It is therefore more difficult to prove that the payments are fraudulent. The discussion of exactly how fraudulent disbursements are made can be found in the sections on Check Tampering and Invoices;

Bid-Rigging Schemes

As we have said, when one person pays a bribe to another, he does so to gain the benefit of the recipient's influence. The competitive bidding process, in which several suppliers or contractors are vying for contracts in what can be a very cutthroat environment, is tailor- made for bribery. Any advantage one vendor can gain over his competitors in this arena is extremely valuable. The benefit of("inside influence" can ensure that a vendor will win a sought-after contract Many vendors are willing to par for this influence.

In the competitive bidding process, all bidders are legally supposed to be placed on the same plane of equality, bidding on the same terms and conditions. Each bidder competes for a contract based on the specifications set forth by the purchasing company. Vendors submit confidential bids stating the price at which they will complete a project in accordance with the purchaser's specifications.

The way competitive bidding is rigged depends largely upon the level of influence of the corrupt employee. The more power a person has over the bidding process, the more likely the person can influence the selection of a supplier. Therefore, employees involved in bid- rigging schemes, like those in kickback schemes, tend to have a good measure of influence or access to the competitive bidding process. Potential targets for accepting bribes include buyers, contracting officials,

engineers and technical representatives, quality or product assurance representatives, subcontractor liaison employees, or anyone else with authority over the awarding of contracts.

Bid-rigging schemes can be categorized based on the stage of bidding at which the fraudster exerts his influence. Bid-rigging schemes usually occur in the pre solicitation phase, the solicitation phase, or the submission phase of the bidding process. The Pre solicitation Phase

In the pre solicitation phase of the competitive bidding process-before bids are officially sought for a project-bribery schemes can be broken down into two distinct types. The first is the need recognition scheme, where an employee of a purchasing company ‘is paid to convince his company that a particular project is necessary. ~e second reason to bribe

EXAMPLE

Gifts and cash payments were given to a majority owner of a company in exchange for preferential treatment during the bidding process. The supplier who paid.the bribes was allowed to submit his bid!' last, knowing what prices his competitors had quoted, or in the alternative, he was allowed to actually see his competitors' bid!' and adjust his own according!)!.

Vendors also bribe employees of the purchaser for confidential information that will help them prepare their bid. Other reasons to bribe employees of the purchaser include to ensure receipt of a late bid or falsify the bid log, to extend the bid opening date, and to control bid openings.

Economic Extortion

Economic extortion cases are the "Pay up or else.. ." corruption schemes; basically the flip side of bribery schemes. Instead of a vendor offering a payment to influence a decision, an employee demands that a vendor pay him in order to. make a decision in that vendor's favour. If the vendor refuses to pay, he faces some harm such as a loss of business with the extorter's company. In any situation where an employee might accept bribes ta favour a particular company or person, the situation could be reversed to. a po.int where ilie employee extorts money from a potential purchaser or supplier.

EXAMPLE

A plant manager for a utility company started his own business on the side. Vendors who wanted to do work for the utility company were forced by the manager to divert some of their business to his own company. Those that did not "play ball" lost their business with the utility.

Illegal Gratuities

Illegal gratuities are similar to bribery schemes except there is not necessarily intent to influence a particular business decision before the fact. In the typical illegal gratuities scenario, a decision is made that happens to benefit a certain person or company. The party who benefited from the decision then gives a gift to the person who made the decision. The gift could be anything of value. An illegal gratuity does not require proof of intent to influence.

EXAMPLE

A city commissioner negotiated a land development deal with a group of private investors. After the deal was approved, the commissioner and his wife were awarded with a fine international vacation, all expenses paid.

At first glance, it may seem that illegal gratuities schemes are harmless as long as the business decisions in question are .not influenced by the promise of payment. But most company ethics policies forbid employees from accepting unreported gifts from vendors. One reason is that illegal gratuities schemes can (and do) evolve into bribery schemes. Once an employee~ has been rewarded for an act such as directing business to a particular supplier, an understanding might be reached that future decisions beneficial to the supplier will also be rewarded. Additionally, even though an outright promise of payment has not been made, employees may direct business to certain companies in the hope that they will be rewarded with money or gifts.

Methods of Making Illegal Payments

Certain traditional methods of making illegal payments fall into the hierarchical pattern described below.

- ✓ Gifts, Travel, and Entertainment

- ✓ Most bribery (corruption) schemes begin with gifts and favours. Commoruyen countered items include:
- ✓ .Wine and liquor (consumable)
- ✓ .Clothes and fewellery for the recipient or spouse .Sexual favours
- ✓ .Lavish entertainment .Paid vacations
- ✓ .Free transportation on corporate jets .Free use of resort facilities
- ✓ .Gifts of the briber's inventory or services, such as construction of home improvements by a contractor

Cash Payments

The next step usually involves cash payments. However, cash is not practical when dealing with large sums, because large amounts are difficult to generate, and they draw attention when they are deposited or spent. The use of currency in major transactions might itself be in c riniin a tin g

Checks and Other Financial Instruments

As the scheme grows, illicit payments are often made by normal busmess check, cashier's check, or wire transfer. Disguised payments on the payer's books appear as some sort of legitimate business expense, often as consulting fees. Payments can be made directly or through an intermediary.

Hidden Interests

In the latter stages of sophisticated schemes, the payer might give a hidden interest in a joint venture or other profit-making enterprise. The recipient's interest might be concealed through a straw nominee, hidden in a trust or other business entity, or merely included by an undocumented verbal agreement. Such arrangements are very difficult to detect, and even if identified, proof of corrupt might be difficult to demonstrate.

Loans

Three types of "loans" often turn up in fraud cases:

- ✓ .A prior outright payment falsely described as an innocent loan.
- ✓ .Payments on a legitimate loan guaranteed or actually made by someone else, .An actual loan made on favourable terms, such as interest~free.

Payment of Credit Card Bills

The recipient's transportation, vacation, and entertainment expenses might be paid with the payer's credit card, or the recipient might forward his own credit card bills to the payer for payment. In some instances, the payer simply lets the recipient carry and uses the payer's card.

Transfers at Other than Fair Market Value

The corrupt payer might sell or lease property to the recipient at far less than its market value, or might agree to buy or rent property at inflated prices. The recipient might also "sell" an asset to the payer, but retain title or the use of the property.

Promises of Favourable Treatment

- ✓ Promises of favourable treatment commonly take the following forms:
- ✓ .A payer might promise a governmental official lucrative employment when the recipient leaves government service.
- ✓ .An executive leaving a private company for a related government position might be given favourable or inflated retirement and separation benefits.
- ✓ .The spouse or other relative of the intended recipient might also be employed by the payer company at an inflated salary or with little actual responsibility.

Red Flags of Bribery Schemes

Most bribery schemes are detected through tips from honest and disgruntled co-workers or vendors. These allegations can be evaluated through analysis of the "red flags" associated with the suspect people or transactions..

The Corrupt Recipient

A person taking payoffs or embezzling funds often exhibits the following characteristics:

The Big Spender—

This is the most common way to detect corrupt recipients; some recipients spend their money. Less conspicuously by paying off debts or paying down mortgages.

The Gift Taker-An official or executive who really accepts inappropriate gifts is often one susceptible to larger payments.

The Corrupt Payer

Like the recipients of bribery payments, the payer will also demonstrate certain identifiable characteristics:

.TheGiftBearer~ The businessperson wsho routinely offers inappropriate gifts, provides lavish business entertainment, or otherwise tries to ingratiate himself is often the one offering still more valuable inducements.

General Purchasing

The following practices may indicate that single (sole) source vendors are being favored, or competitive bidding policies are not being followed: Materials are not being ordered at the optimal reorder point .Orders is consistency made from the same vendor. .Established bidding policies are riot being followed. .The costs of materials are out of line..

Presolicitation

Restrictions in an organization's solicitation documents that tend to restrict competition are a red flag. Examples of restrictive conditions include:

- .Specifications and statements of work that are tailored to fit the products or capabilities of a single contractor.
- ."Prequalification" procedures that restrict competition.

- .Unnecessary sole-source or noncompetitive procurement justifications: -Containing f~se statements
- -Signed by unauthorized officials
- -Bypassing necessary review procedures

Other red flags in the presolicitation phase include:

- ✓ .A buyer who provides information or advice to a contractor on a preferential basis. .New vendors that are added to the "qualified" list for rio apparent reason.
- ✓ .Statements of work, specifications, or sole-source justifications that are developed by, or in consultation with, a contractor who will be permitted to bid.
- ✓ .Consultants who assisted in the preparation of the statements of work, specifications, or design, and are later permitted to work on the contract as subcontractors or consultants.
- ✓ .Projects that are split into smaller contracts to avoid review.
- ✓ Information that is released by f1rnls participating in the design and engineering to contractors competing for the prime contract.
- ✓ .Requirements that are split up so contractors can each get a "fair share" and can rotate
- ✓ bids.
- ✓ .Specifications that are not consistent with similar procurements in the past.

Bid Solicitation

The following are examples of suspicious activity that might signal fraud in the bid solicitation phase:

- ✓ .The time for submitting bids is limited so that only those with advance information have adequate time to prepare bids or proposals.

- ✓ .One contractor receives confidential information that is not revealed to his competitors.. .The conducting of a bidders' conference, which permits improper communications
- ✓ Between Contractors, who then are in a position to rig bids.
- ✓ .The failure to ensure that a sufficient number of potential competitors are aware of the solicitation by:
- ✓ -Using obscure publications to publish bid solicitations -Publishing bid solicitations during holiday periods
- ✓ .Bid solicitations that is vague as to the time, place, or other requirements for submitting acceptable bids.
- ✓ .Inadequate internal controls over the number and destination of bid packages sent to interested bidders.
- ✓ .Improper communication between purchasers and contractors at trade or professional meetings.
- ✓ .Improper social contact between purchasers and contractor representatives.
- ✓ .A purchasing agent who has a financial interest in the business of a contractor. .A purchaser who discusses possible employment with a contractor. .The purchaser assisting a contractor in the preparation of his bid.
- ✓ .A contractor being referred to a specific subcontractor, expert, or source of supply by an employee of the purchasing organisation.
- ✓ .The failure to amend a solicitation to include necessary changes or clarifications in the bid, such as telling one contractor of changes that can be made after the bid.
- ✓ .The falsification of documents or receipts so that a late bid is accepted. .Any indications of collusion between bidders.
- ✓ .The falsification of a contractor's qualifications, work history, facilities, equipment, or personnel.

Cash Receipting Fraud Schemes

Skimming

Skimming currency from customer payments is quite simple. That's why it's the crime of choice and the most common form of cash receipts fraud. The actual amount of losses from skimming is unknown, and most schemes are not detected. The primary suspect is a cashier. The cashier merely has to talk customers out of a receipt or give them a bogus cash receipt form for any transaction for services rendered by the organization. Either method works if the customer isn't concerned by either of these conditions and if the organization hasn't implemented internal controls over the revenue sources at this location. Business continues normally, and everything appears to be just fine. But it isn't.

To detect this type of fraud, listen to what cashiers say when they interact with customers. The highest risk question from any cashier is: "Do you need a receipt?" If the customer says "yes," the cashier receipts the transaction and is then accountable for the funds. If the customer says "no," or if the casher gives the customer a bogus cash receipt form, the funds received from these transactions basically represent "free" money, because there was no accountability established for the revenue from this transaction. Using video cameras in the cashier area helps to deter skimming by cashiers. Using some alternative method of determining sales (such as the number of units sold times unit price equals revenue) also works, but with limited success in retail businesses where there are too many variables in unit prices. Getting sales recorded is the issue.

Cashiers operating cash registers anywhere, such as at restaurants, bars, coffee houses, and retail sales establishments, often operate with an open cash drawer. When customers make payments for purchases, cashiers merely make change. The amount of money received from these sales is simply stolen. This is skimming of currency from customer payments at its best. And it's happening every day of the year in businesses all over the world. It's the primary reason business try to separate cash receipting from product delivery, such as in fast food restaurants.

The same thing also happens when a customer makes a payment with a check. Sometimes a cashier will tell a customer to leave the payee area on the check blank because he or she has a

rubber stamp with the organization's name. A crooked cashier will write his or her name or the word "cash" on the payee line of the checks and either cash them at a financial institution, or deposit them into his personal bank account. Sometimes the cashier will tell customers that their canceled checks are their receipts or those receipts aren't issued at the facility. When these check transactions aren't receipted, a crooked cashier often substitutes them for cash that has been received and recorded from other transactions on the same business day (i.e.; a check for cash substitution scheme). The cashier easily removes an equal amount of currency from the cash register till drawer at any subsequent time during the day and keeps the money for personal use.

These losses hit the organization's bottom line immediately. Indications of these irregular activities later appear in inventory shortages that are written-off as expenses and then decrease the organization's net income. Rarely do these fraudulent activities force an organization into bankruptcy or put them out of business. But the reduced amount of revenue from operations certainly does hurt the organization's overall financial picture. Also, the government doesn't receive sales tax from these unrecorded transactions. Consumers actually pay a theft tax for skimming losses, shoplifting by customers, and the theft of merchandise by employees in the form of higher retail prices.

Skimming currency from customer payments for services rendered by the organization most often occurs at a decentralized location where there is only one employee on duty. In such circumstances, there is no one present to observe how transactions are handled or to independently determine if all transactions have been processed as required. But, cashiers at central treasury facilities use the same methods that employees use to skim revenue at decentralized locations. However, because of the number of employees involved at these facilities, managers normally implement internal controls over cash receipts by segregating duties among employees and instituting improved cash receipting systems for all funds received.

These funds include payments from customers and all money transmitted to the central treasury facility by decentralized locations. However, even these procedures don't deter an unscrupulous cashier from skimming currency.

A customer rarely "sees" the fraud involving their transaction because the process is so relaxed and comfortable. The customer wants the transaction completed quickly with minimal disruption of their life so he or she can resume their daily routine. A crooked cashier knows this and simply smiles while telling the unsuspecting customer to have a nice day. As soon as the customer\ departs the facility, the cashier steals the funds.

The revenue sources employees choose for skimming include all types of miscellaneous revenue that aren't controlled by accounts receivable systems. Even though managers know this scenario provides an incentive for unscrupulous employees to steal funds, they often don't implement internal controls to protect the revenue sources generated throughout the organization. From time to time, even some honest employees are tempted and cross over the line from being honest to becoming dishonest.

Case Study: King County Solid Waste Division - $162,500

Four cashiers and machine operators skimmed at least $162,500 in revenue from the Hobart Landfill site during a one-year period. The investigation by the internal auditor included the use of covert surveillance techniques (i.e.; videotape cameras) to record the cash receipting activities of landfill employees and analytical procedures on the historical cash receipting activity of individual landfill cashiers. The loss was covered by the county's insurance bonding policy. Three employees were sentenced to three months in the county jail. The fourth employee was sentenced to two months in the county jail.

Check for Cash Substitution Scheme

A check for cash substitution scheme is the primary way funds are stolen in any cash receipting activity. This scheme is perpetrated by a cashier or accounting clerk who substitutes checks from unrecorded payments for cash from payments which have been receipted and recorded in the accounting records. When the cashier places the checks from these unrecorded transactions in the cash drawer, there is an immediate overage in the account. To remedy this situation, the cashier merely removes the displaced cash from the cash drawer. These funds are simply stolen.

In the state of Washington, this scheme accounts for 10% of all fraud cases, but 25% of the dollar losses ($4 million over 20 years). This is the crime of choice for a supervisory cashier, one who makes the bank deposit without anyone ever looking at its composition.

The prime suspect is the person who makes the bank deposit. You have to pay attention to this scheme.

Substituting checks for cash, dollar for dollar, is the most common method used by cashiers to misappropriate funds. Substituting checks for cash on less than a dollar for dollar basis is not quite as simple, and isn't done as often. In these cases, the full amount of the check is deposited in the bank, while a receipt is issued for any amount less than the amount the customer actually paid.

The checks used in this scheme are almost always received through the mail. These are high risk transactions because these customers do not ever expect to receive a receipt. Their canceled check is their receipt. The customer's account for each unrecorded transaction is always marked "paid".

Case Study:

Affiliated Health Services (Hospital) - $213,668 – 3Years Scheme. A general ledger technician committed a check for cash substitution scheme to manipulate the hospital's daily bank deposit. Decentralized locations at two hospital district recorded mode of payment on cash receipts issued and summarized this information on daily accountability reports for cash collections. Some of these locations did not issue cash receipts for certain types of collections. But, all funds were transmitted to the central administrative office where the bank deposit was prepared. The employee kept unrecorded revenue checks from these areas in her desk ($48,000 at the time of our audit). These checks were then substituted for currency received from the cafeteria, the primary location receiving currency each day. No one verified the check and cash composition of the daily bank deposits or otherwise monitored the work of this technician.

Detection. Routine SAO audit in cash receipts testing and review of the hospital's internal controls over cash receipts. The check and cash composition of the daily bank deposits did not

agree with the mode of payment on the cash receipts issued by the decentralized hospital locations. There were more checks and less currency in the bank deposits, the primary attribute of a check for cash substitution scheme.

Internal Control Weaknesses (Red Flags).

Policies and procedures were circumvented.

(1) Segregation of duties problem. The general ledger technician gained access to the hospital's mail and computer records over time (job creep). In addition to her duties in preparing the bank deposit where she had access to all hospital revenue, she also had access to patient and other hospital billing records where she had authority to process account adjustments. Her work was not properly supervised by managers.

(2) The district did not properly control checks which arrived through the mail, and internal controls over cash receipts were inadequate. No one compared the mode of payment from the cash receipts issued and daily accountability reports to the check and cash composition of the daily bank deposit for agreement.

(3) There was very little cash in bank deposits; but, large amounts of currency were routinely received from the hospital cafeteria.

(4) Checks were not always receipted at the point of entry at all of the hospital's decentralized operating locations.

(5) Miscellaneous commercial account adjustments were not promptly review by managers.

Detection Steps.

(1) Review employee duties to determine if one individual is able to control transactions from beginning to end, particularly in the cash receipting function. Determine whether managers review the work of the person preparing the bank deposit in the same way the employee reviews the work of others.

(2) In cash counts and cash receipts testing, compare mode of payment information from daily accountability documents to the check and cash composition of the daily bank deposit.

(3) Review accounts receivable adjustments to determine if they are authorized, approved, and properly supported. Determine if an exception report is prepared for all account adjustments for management oversight purposes.

(4) Review procedures for processing mail. Determine if two people open the mail, make a list/log of all checks received, and then compare the amount of revenue received to subsequently prepared cash receipt and bank deposit records.

(5) Perform analytical reviews of revenue streams and miscellaneous revenue for reasonableness and agreement with expectations.

Sentencing. The general ledger technician pleaded guilty to first degree theft and was sentenced to one year in jail at the Washington State Department of Corrections at Purdy. Exceptional sentencing guidelines were used.

Training Example

The attached case example clearly demonstrates how a review of the composition of a daily deposit will detect a check for cash substitution scheme. While this is not an actual fraud case, all frauds look exactly like this.

There were 3 receipts issued on the date in question, January 15, 1988. The receipts used are official pre numbered receipts which indicate mode of payment information, and were issued in numerical sequence. These represent 100% of the transactions for this date. Each transaction represents $1,000 in cash receipts. Two of these transactions were paid by cash (Jones and

Adams), and one transaction was paid by check (Smith). Take the following steps:

Add up the total amount of cash receipts for this date ($3,000) and agree this to the deposit total ($3,000). Since these amounts agree, this organization deposits cash receipts intact daily. If this is where your cash receipts testing normally ends, you're making a serious mistake. If you stop here, you've missed the fraud! The cashier you're auditing will now be able to continue perpetrating this scheme in this organization. So, don't let this happen to you. Keep going!

Add up the amount of cash (i.e.; currency) received for the day ($2,000). Compare this amount to the actual cash deposited for this date ($1,000). If these amounts agree, your composition review is finished. If not, you have additional audit work to perform. In this case, the amount of cash deposited ($1,000) was less than the amount of cash received from the recorded cash receipts ($2,000). Thus, on this date, there is an unreconciled difference of $1,000 (more cash was received than was deposited). When these variances occur, you must analyze the actual checks recorded on the deposit slip to determine which checks do not belong there. In a fraud case, this will identify the universe of unrecorded cash receipt transactions which have been included in the deposit on this date.

In this case, the check for Smith is properly shown on the deposit slip. But, the check for

James does not belong in this deposit. There was no cash receipt written for James on this date.

Contact the organization's bank. Request a copy of the check for James from the bank's microfilm record of deposits so that additional audit work can be performed. It is not necessary to order copies of all checks shown on the deposit slip for days with variances.

Once the check for James is obtained from the bank, you need to determine why it was included in the subject deposit. The fact that the check is located in the deposit does not necessarily mean that fraud exists. There could be a valid reason for this condition.

If a fraud is not involved, the check may be from one of the following sources:

(a) a personal check cashed by an employee or other individual;

(b) a check from another source of revenue commingled with this deposit (the fraud may be in another function);

(c) a check for an amount greater than a legitimate customer payment (i.e.; less than $10 over the amount due on the account); or

(d) some other miscellaneous valid and explainable reason, such as an error made inrecording the mode of payment on the cash receipt form.

Items (a) and (c) above must have an organization policy covering the conditions under which these situations will be permitted.

If a fraud is involved, the check represents an unrecorded payment made by a customer (check for cash substitution scheme). In an accounts receivable operation, your additional research will indicate that the customer's account (individual subsidiary ledger card) has been marked "paid" for the transactions in question. In a municipal or district court, the customer's traffic citation for this transaction will be marked "paid" (perhaps by canceling, voiding, dismissal, etc.) and filed in the completed file. In this example, the extra check for James does, in fact, represent an unrecorded transaction. Thus, the cashier in this organization is operating a check for cash substitution scheme.

Compute the amount of the loss as follows: First, determine the correct amount of total accountability for this date. In this example, you must add the unrecorded transaction for James ($1,000) to the total of the recorded transactions for Jones, Adams, and Smith ($3,000) to determine total accountability ($4,000). Next, subtract the amount of the daily deposit ($3,000) from the correct total accountability ($4,000). Finally, this calculation gives you a difference of $1,000 which represents the cash shortage in this account. Therefore, this example involves a fraud where $1,000 in public funds was stolen by a cashier on this date.

Lapping Scheme

A lapping scheme can be perpetrated in any cash receipting activity; but, it's most often associated with an accounts receivable function. This scheme is perpetrated by a cashier or accounting clerk who issues cash receipt forms for customer payments, but subsequently makes no bank deposit, or a short bank deposit, of the funds. The difference between the total amount receipted and the lesser amount deposited is stolen (borrowed). Cumulative cash shortages over a period of time represent the total amount of the loss in a lapping scheme. The customer's account for each unrecorded transaction is always marked "paid".

Lapping schemes are perpetrated at decentralized cash receipting locations where funds are initially received from customers, and at the central treasury function after funds have been transmitted there for subsequent deposit in the bank. This type of cash receipts fraud is not very

smart (i.e.; dumb), because the inevitable day of reckoning comes when the perpetrator realizes that the lapped amount must be disposed of in some manner before they are detected.

Types of lapping schemes.

Simple. While all cash receipt transactions are receipted by the cashier each day, funds received on a subsequent date are used to cover the initial shortage. The cumulative amount of the loss is systematically rolled through the accounts.

Complex. Cash receipt forms are not necessarily issued for all customers payments, such as for checks received through the mail. Funds received today are first stolen. Then, funds received on a subsequent date are used when cash receipt forms are issued covering the amount of the previously omitted transactions. Funds received from customer "B" are credited to the account of customer "A". The perpetrator must keep an accurate record of the transactions which have not been recorded (or have been inaccurately recorded) in the accounting records because the cashier or accounting clerk must post payments to these accounts in a sufficient amount of time to prevent customer feedback from delinquent billing notices.

Lapping Scheme Training Example

The following is an example of a lapping scheme fraud which uses three customers who each owe $100 in an organization's accounts receivable system:

Customer "A" pays $100. An employee misappropriates these funds. The $100 loss of funds remains with this customer.

Customer "B" pays $100. This payment is credited to the account of Customer "A" who is made whole by this transaction. Now, the $100 loss of funds remains with this customer.

Customer "C" pays $100. This payment is credited to the account of Customer "B" who is made whole by this transaction. Now, the $100 loss of funds remains with this customer.

The loss begins with Customer "A", but ends up with Customer "C".

The "net cumulative effect" of these account manipulations is that an employee has misappropriated a $100 payment from Customer "C". It is the sole remaining account that has

not been credited with the proper payment. A list of these accounts must be prepared to provide the amount of loss in the case. Attempting to find all of the manipulated accounts in the scheme is fruitless.

Fraud perpetrators must maintain accurate records in order to conceal the irregular activity.

Mistakes ultimately bring down these schemes. It just takes one valid customer complaint to bring down the scheme. Disaster then strikes with devastating results.

An important issue is that an independent party must resolve all customer feedback (complaints).

This is essential for fraud detection purposes.

Ways perpetrators conceal the disposition of lapping scheme losses

There are a number of ways fraud perpetrators attempt to conceal the disposition of lapping schemes. Some of them include:

Making restitution or pay back the amount of the loss, either secretly or by informing the organization.

Canceling the accountability established by the cash receipts issued, such as by unauthorized voiding activity.

Destroying the supporting documents representing the accountability for the funds stolen.

Reporting a mysterious disappearance theft of cash receipts. This is a bold attempt to conceal the losses of any lapping scheme.

Accounts Receivable Fraud Schemes

Accounts Receivable – Internal Control Structure - Duties of Personnel

The ideal separation of duties for employees working in the accounts receivable function is as depicted in the diagram shown below. Three employees are needed. But, this is not always possible. Therefore:

If one person performs all duties in the function, someone independent of the employee must monitor their work.

If two employees perform all duties in the function, their duties should be split between billing and posting the accounting records and collecting and depositing funds. But, someone independent must perform the reconciliation of account postings and bank deposits. If this is not possible, the employee performing the billing and posting duties should also perform the reconciliation (least risk) rather than the employee collecting and depositing funds (highest risk).

Types of Accounts Receivable Fraud Schemes

Manipulations in "on-book" accounts receivable frauds include at least the following types of schemes:

Check for Cash Substitution Schemes.

Perpetrators steal unrecorded checks from non-accounts receivable revenue streams (i.e., miscellaneous revenues or one-time charges) and exchange them for cash in an equal amount from accounts receivable transactions that have been recorded in the accounting system.

When this occurs, the check and cash composition of the bank deposit will not agree with the mode of payment (i.e.; check or cash) of all cash receipt transactions for each business day.

The cash is simply stolen.

Lapping Schemes.

In this most common scheme in the accounts receivable function, a perpetrator first steals customer A's payment and then applies customer B's payment to customer A's account balance. To prevent managers and customers from discovering these manipulations, the fraudster must keep accurate records of all accounts involved in the scheme. These records normally are maintained somewhere in the employee's office or desk. The perpetrator rationalizes that the money is only being borrowed and intends to make full restitution later.

But, as the size of the scheme increases over time, employees soon realizes that it will be impossible to replace the money. They stop keeping records, but must ensure that all

manipulated accounts have been properly credited by the end of the billing cycle. This is a stressful juggling act that often requires the fraudster to come to work early and stay late.

They need this quiet time to conceal the scheme from managers and be present in the workplace to respond to any customer complaints. One of their biggest fears is being absent from the workplace because that's when the risk of detection is highest. We're always thankful for the inevitable family emergency that comes along because many accounts receivable schemes are uncovered when another employee performs the fraudster's job and discovers the irregularities. Eventually, the perpetrator can't manage the scheme because of the amount of the loss and the number of accounts they're manipulating. The scheme begins to unravel, and this is when mistakes are made. To avoid this, fraud perpetrators often conceal losses in delinquent or slow-pay accounts.

Other Accounting Manipulations

A perpetrator manipulates accounting records by recording a smaller amount of cash receipts in the control account (which agrees with the daily bank deposit total) than is recorded on the subsidiary ledger cards for all customer payments. This causes an imbalanced condition between the control account balance and the total of the balances on all subsidiary ledger cards. We receive frequent inquiries from financial managers who want to know how an employee could possibly record different amounts in these records. This is a one-sided transaction, that's for sure. Many times managers or auditors discover these conditions and simply write-down the control account balance by using unsupported adjustments to make it agree with the total of the subsidiary account balances. They do this because they just can't seem to find a reasonable explanation for this unusual condition. However, these adjustments simply eliminate the accountability for any missing funds. These adjustments are only made when no one has been able to detect a fraud that's in progress. If someone detects a fraud, the managers or auditors obviously would take different actions.

These unsupported adjustments eliminate accountability for the missing funds and help to mask or conceal the scheme for long periods of time. Some say their organization's computers will prevent this from happening. But it's still possible to perpetrate these fraud schemes without

detection. Often, managers are so trusting that they fail to monitor the critical accounting reports that clearly show what's happening within their operations.

Eliminating Customer Accounts

In certain organizations, such as those that provide utilities, a dishonest employee in the accounts receivable function can disregard the debts of some customers. These can include the fraudster's own account or those of their relatives or other employees who are their friends. The employee may eliminate the accounts from the accounts receivable billing system or store the subsidiary ledger cards for those accounts in a separate file. These offline accounts are never billed by the organization. Thus, services are "free". In a utility, the customer books are the original source documents that prove the universe of all accounts in existence. In other organizations, the master list of all credit cards issued to customers serves the same purpose.

When dealing with this type of fraud in the past, our major focus was on the employees who performed the computer input function after the utility meters were read and documented by other employees. But, we've now shifted this focus to others in the organization because many utilities are using hand-held equipment that electronically uploads meter readings directly into the computer. This helps prevent fraud in the input process. However, stubborn fraudsters simply find new ways to do business.

Fictitious Account Adjustments

Legitimate account adjustments in accounts receivable include: (a) pre-billing adjustments for unusual circumstances, such as meter reading errors and broken transmission lines or facilities; and, (b) post-billing adjustments for other miscellaneous accounting errors noted by both employees and customers for a wide variety of reasons. Account adjustments in delinquent accounts usually totally eliminate a debt.

However, unsupported account adjustments simply eliminate the accountability for money from real debts owed to the organization after customer payments have been stolen. These adjustments represent a high risk for fraud, similar to any other kind of negative cash transaction. All computer accounting systems should, but don't always, produce exception reports that identify

the universe of the customer account adjustments processed each business day. And, even if such reports are produced, managers often don't adequately monitor these high-risk operations. Account adjustment fraud schemes aren't always perfect, but they do represent some of the more memorable cases we've ever encountered.

Stealing the Statements

Some perpetrators who steal customer payments don't have the ability to write-off account balances. Thus, these employees are forced to resort to "stealing the statements" of customers with invalid delinquent account balances to conceal that they've misappropriated the funds from the payments made by these customers. They do this inside the organization before the statements are mailed and outside the organization after the statements have been mailed. In both scenarios, customers receive manually prepared statements indicating that they owe only amounts due from charges in the current billing period. The fraud perpetrator must then conceal the delinquent account balances from managers and customers.

These schemes are almost always doomed to failure because eventually the organization is going to send a delinquency notice to a customer who responds by saying, "My account isn't delinquent, and I paid my bill." They then produce cash receipts or canceled checks to prove this condition. An independent customer service department must carefully listen to customer complaints and research each problem thoroughly. If a cashier or accounting clerk who manipulated the account is also responsible for responding to these inquiries, they often tell customers that the organization is experiencing computer problems. They then make fictitious account adjustments that conceal the irregular activity. This enables them to correct their mistakes and keep the scheme active for long periods of time. These schemes are often complex and very interesting.

Method of Documenting Accounts Receivable Losses

Once fraud has been detected in the accounts receivable function, we make sure that the organization separates the suspect employee from the accounting records. Most employees are simply placed on administrative leave while the fraud investigation is conducted so that they

can't continue to manipulate the accounting records. We just let the computer send out customer statements without any outside intervention.

We use computerized billing statements, depicting all balances owed by customers, as the most common method to determine the total amount of the loss in an accounts receivable scheme.

Customers' complaints about irregularities identify the universe of all manipulated accounts.

We ask the organization to maintain a master log of all complaints and resolutions after it compares customers' records of account payments to information in the computer system. The organization must obtain copies of supporting documents from customers for any unrecorded payments. These supporting documents must be maintained on file to support any account adjustments and for audit purposes. We then verify the accuracy of this tabulation.

Major Areas of Concern in Accounts Receivable Systems

The main issue in a utility accounts receivable fraud case is that someone in a utility operation is going to steal cash receipts (currency or checks). Once this is done, the employee will do whatever they are able to do (i.e.; what they are able to control) to keep the fraud from being detected by management or auditors. For example:

Problem: When employees steal a customer's payment, they have to make the account "right" or suffer the resulting customer feedback. The employee must do one of two things in order to conceal the irregular activity. They either write-off the account, such as through a "non-cash credit" transaction (i.e.; an account write-off, adjustment, or cancellation), or let the account go delinquent (i.e.; without taking any action).

This latter condition is very dangerous and usually results in customer feedback and detection of the scheme. It's extremely important for all customer feedback to come to an independent party or function for proper research. Customer feedback should not come back to the accounts receivable function where a dishonest employee will further manipulate the records to conceal any irregular activity from view by managers.

Solution: Management reviews and audit tests in utility accounts receivable operations must focus on these two alternatives available to cashiers. The accounts receivable accounting system

should produce an “exception” report at the end of each business day listing the universe of all “non-cash credit” transactions. Each transaction should be authorized and approved, and be supported by appropriate documentation for the action. Delinquent accounts should also be monitored closely. Customer account confirmations should be considered.

The next most common attribute auditors see in utility accounts receivable fraud cases is that the total amount of customer payments is more than the total amount of the bank deposits.

Therefore, we should always perform this test. And, an independent party from cashiering and account maintenance should routinely reconcile this information.

When accounts are written-off, we need to review the exception report that lists the universe of all such transactions to determine whether all write-offs have been authorized and approved as well as properly supported. Typically, employees have no support for fictitious write-off transactions. We often forget that employees who have the ability to process such transactions always have the ability to do this 24 hours a day, 7 days a week, 365 days a year, whether it’s authorized or not. Therefore, the “exception” report is mandatory for use as a monitoring tool in the accounts receivable system.

For delinquent accounts, we should confirm significant outstanding account balances with customers. But, when fraud is involved, why doesn't the customer know? The answer to that question is that an organization employee has purposefully suppressed this information from view. Customers are placed on "no bill" status or are receiving manual bills from the utility showing charges from only the current period (stealing the statements). We should review the computer list of all accounts not billed to ensure that the justification for each such account is appropriate. We should also review the computer list of all accounts scheduled for “shut-off” to ensure that customer services were terminated as required by law.

Knowing what miscellaneous revenue streams exist at the utility is also extremely important.

These revenue streams are the primary targets of cashiers because there often are few accounting records that help anyone identify the universe of these transactions. In addition, the cash receipting systems that exist to account for and document these revenues are often deficient.

In addition, we should always review the amount of cash in utility bank deposits to determine if it is reasonable based upon the collective knowledge of managers and auditors. When frauds occur, cash is conspicuously missing from the bank deposits.

Determine if there is any (or a sufficient amount of) cash in the daily bank deposits.

Steps to Detect Fraud in Accounts Receivable Systems

Step Number 1. As of a specific cut-off date, agree (compare) the balance in the accounts receivable control account to the total of the customer account balances recorded on the subsidiary ledger cards in the file.

Step Number 2. For a specified accounting period (i.e.; day, week, month, or year), agree (compare) the total of all credits recorded on the subsidiary ledger cards in the file to the: (a) total cash collections posted to the control account; (b) total bank deposits; and, (c) total cash receipt forms issued or total collection stubs on file, depending upon the accounting system used.

When comparing total credits to customer accounts to related bank deposits and using this as an analytical procedure, remember that this is also a substantive audit test. Deposit shortages represent losses of funds.

Step Number 3. Where possible, such as in a utility accounts receivable system (i.e.; water, sewer, electricity, garbage, etc.), agree (compare) the total number of all customer books (i.e.; meter, route, location, etc.) to the total number of active subsidiary ledger cards in the file or active customer accounts on a computer system. Think universe. Review the propriety of all customer accounts included on a "no bill" report. Determine if the organization ensures that all new accounts (e.g.; meters) are effectively communicated to utility billings. In a customer credit card system, agree (compare) the total number of credit cards issued to the total number of subsidiary ledger cards in the file.

Step Number 4. Review accounts receivable credits (i.e.; cancellations and adjustments), with emphasis on transactions which affect the accounts of employees and their relatives, and transactions that affect only the control account. Review customer accounts receivable write-offs for propriety. Determine if the organization has an exception report listing the universe of these

high risk transactions, and whether all adjustments are approved and properly supported. Again, think universe.

Step Number 5. As of a specific cut-off date, confirm all delinquent customer accounts receivable balances if significant or warranted. When irregularities occur, employees sometimes divert customer billing statements to themselves, such as by changing the mailing address to their own address or to a post office box they control. Sometimes delinquent accounts balances are manipulated and billing statements sent to customers showing no balance due from prior periods. These irregularities are called "stealing the statements".

Step Number 6. Review billing rates for propriety. Analyze all flat (standard) fee or rate customer accounts. Test actual billing rates to the authorized billing rate established by resolution, ordinance, or other authorized rate structure.

Step Number 7. Determine whether the organization knows the percentage of their customer payments that are made in cash, and whether this expectation is being met. Determine if there is any (or a sufficient amount of) cash in the daily bank deposits.

Typical Accounts Receivable Fraud Scenario

Warning: Watch out for documents that eliminate the accountability for cash receipts in manual or computer systems (cash registers).

The Fraud: Unauthorized transactions are processed for:

Voids, Paid-outs, and Refunds (Every Organization)

Non-cash credits (Primarily in Courts, but also College Scholarships)

Cancellations (Accounts Receivable Systems-Utilities)

Adjustments (Accounts Receivable Systems-Utilities)

Any Account Write-Off (Accounts Receivable Systems-Utilities)

For every use of these transactions types, there can also be an abuse.

Prevention: Supervisory approval and monitoring is required for these transactions.

Use specific forms for these purposes.

Retain all copies of supporting documents on file.

Prepare exception reports for these transactions types.

Review "no bill" and "shut-off" customer account reports.

Monitor the activity of these high risk transactions.

Common Problem: No (or little) cash in daily bank deposits.

Does the organization know the percentage of their customer payments that are made in cash?

We normally hear everything from 5% to 20% of the total bank deposit/revenue. But one city recently reported the number exceeded 50% because of a change in the population demographics. The question is: What is right for each operation? And, does the organization periodically review their records to see if their expectations are being met?

Does the organization know which customers pay their account in cash? These accounts might also be "flagged" in some way for identification purposes within the organization's computer system. The organization should require an exception report of any adjustments made to these accounts because they are the highest risk accounts. These are the accounts most often manipulated by employees.

Common Failing: Managers often forget that when an employee's job duties include processing adjustments to customer accounts, this employee always has the ability to process adjustments to customer accounts, whether these actions are authorized or not. Employees simply process unauthorized adjustments to conceal irregular activity from view. An exception report is required (think universe).

Other Cash Receipting Fraud Schemes

There are, of course, many other cash receipting fraud schemes. However, there would never be enough time for us to cover then in any detail. So from my life experience dealing with fraud in the state of Washington, some limited coverage of these fraud schemes is presented below:

Cash register schemes (voids, refunds, paid-outs, and missing "Z" tapes).

Computer cash receipting schemes (non-cash credit transactions, such as community service and jail time in courts).

Placing personal checks in the till drawer (borrowing schemes, where all fraud starts). Establishing your own accountability (the most dangerous person in any organization)

Altering cash receipt forms after issue (identifying the attribute of ink versus carbon on the accounting copy of receipts issue is the key to detection of these schemes).

Multiple cash receipt books (one for the organization and one for the cashier - finding them is critical to detection of these schemes).

Making short bank deposits (this is more common than you might think–account for the universe of all revenue transactions).

"Free" access to safes and vaults (no fixed responsibility for funds is the issue).

Not requiring decentralized locations to make direct bank deposits (transmittal systems must be secure).

Retail sales activity (normally present in schools, but applicable to retail sales operations in any organization)

Checking account schemes (cashing entity revenue checks and taking "cash back" from an official bank deposit – money laundering is the issue).

Establishing bogus organization checking accounts (misappropriation of revenue by money laundering is the issue)

ASSET MISAPPROPRIATION: INVENTORY AND OTHER ASSETS

Employees target inventory, equipment, supplies, and other non-cash assets for theft in a number of ways. These schemes can range from stealing a box of pens to the theft of millions of dollars worth of company equipment. The term inventory and other assets is meant to encompass the misappropriation schemes involving any assets held by a company other than cash.

Misuse of Inventory and Other Assets

There are basically two ways a person can misappropriate a company asset the asset can be misused or it can be stolen. Simple misuse is obviously the less egregious of the two. Assets that are misused but not stolen physically include company vehicles, company supplies, computers, and other office equipment.

EXAMPLE An employee made personal use of a company vehicle while on alt out-of town assignment. The employee provided false information, both written and verbal regarding the nature of his use of the vehicle. The vehicle was returned unharmed and the cost to the perpetrator's company was only a few hundred dollars. Nevertheless, such unauthorized use of a company asset does amount to fraud when a false statement accompanies the use.

One of the most common examples of the misuse of company assets occurs when an employee uses company equipment to do personal work on company time. For instance, an employee might use his computer at work to write letters; print invoices, or do other work connected with a business he runs on the side. In many instances, these side businesses are of the same nature as the employer's business, so the employee is essentially competing with his employer and using the employer's equipment to do it.

The Costs of Inventory Misuse

The costs of inventory misuse are difficult to quantify. Too many individuals this ~e of fraud is not viewed as a crime, but rather as "borrowing." In truth, the cost to a company from this kind of scheme is often immaterial. When a perpetrator borrow: a stapler for the night or takes home

some tools to perform a household repair, the cost to his <;ompany is negligible, as long as the assets are returned unharmed.

On the other hand, misuse schemes could be very costly. Take, for example, the situation discussed above in which an employee uses company equipment to operate a side business during work hours.. Since the employee is not performing his work duties, the employer suffers a loss in productivity. If the low productivity continues, the employer might have to hire additional employees to compensate, which means more capital diverted to wages. If the employee's business competes with the employees, then lost business could be an additional cost. Unauthorized use of equipment can also mean additional wear and tear, causing the equipment to break down sooner than it would have under normal business conditions. Additionally, when an employee "borrows" company property, there is no guarantee that he will bring it back. This is precisely how some theft schemes begin. Despite some opinions to the contrary, asset misuse is not always a harmless crime.

Theft of Inventory and Other Assets

While the misuse of company property might be a problem, the company property is obviously of greater concern. Losses resulting from larceny of company assets can run into the millions of dollars. Most schemes where inventory and other non-cash assets are stolen fall into one of four categories: larceny schemes, asset requisition and transfer schemes, purchasing and receiving schemes, and false shipment schemes.

Larceny Schemes

The textbook definition of Larceny is "Felonious stealing, taking and carrying, leading, riding, or driving away another's personal property, with intent to convert it or to deprive owner thereof. The unlawful taking and carrying away of property of another with intent to appropriate it to use inconsistent with latter's rights"* this definition is so broad; it encompasses every kind of asset theft. In order to gain a more specific understanding of the methods used to steal inventory and other assets, the definition of larceny has been restricted. For the purposes of classifying asset misappropriations, the term larceny is meant to refer to the most basic type of inventory theft, the schemes in which an employee simply takes inventory from the company premises without

attempting to conceal the theft in the books and records. {See "Non-cash Larceny" flowchart.) In other fraud schemes, employees may create false documentation to justify the shipment of merchandise or tamper with inventory records to conceal missing assets. Larceny schemes are blunter. The culprit in these crimes takes company assets without trying to "justify" their absence.

Non-cash Larceny

Most non-cash larceny schemes are not very complicated.. They are typically committed by employees with access to inventory or supplies. Many employees simply carry company assets away in open view of other employees. People tend to assume that their friend's arid acquaintances are acting honesty. When they see a trusted coworker taking something out of the workplace, most people assume that the culprit has a legitimate reason for doing so.

EXAMPLE A university faculty member was leaving his offices to take a position at a new school this person was permitted to take a small number of items to his new job, but certainly exceeded 1he intentions of the school when he loaded two tricks university lab equipment and computers worth several hundred thousand dollars. The perpetrators simply packed up these stolen assets along with his personal item and drove away.

Unfortunately, in all too many cases the coworkers of the perpetrator are fully aware that he is stealing company assets, yet they refrain from reporting the crime. There are several reasons that employees might ignore illegal conduct, such as a sense of duty to their friends, a "management vs. labour "mentality, poor channels of communication for whistleblowers, or intimidation of honest employees by the thief. When high-ranking personnel are stealing from their companies, employees often overlook the crime because they fear they will lose their jobs if they report it. In some cases, the coworkers may be assisting in the theft.

EXAMPLE

A school superintendent was not only pilfering school accounts but was also stealing school assets. A search 0/ his residence revealed a cellar filled with school property. A number 0/ school

employees knew or suspected the superintendent was involved in illegal dealings, but he was very powerful and people were afraid to report him for fear 0/ retaliation. As a result, he was able to steal from the school for several years.

Ironically, employees who steal inventory are often highly tr1isted within their organizations. Because these employees are trusted, they may be given access to restricted areas, safes, supply rooms, or other areas where company assets are kept. This access makes it easy for these employees to steal.

It can be unwise for an employee to physically carry inventory and other assets off the premises of his company. This practice carries with it the inherent risk and potential embarrassment of being caught red-handed with stolen goods on his person.

The False Sale

In many cases, corrupt employees utilize outside accomplices to help steal inventory. The fake sale is one method that depends upon an. accomplice. Like most inventory thefts, the fake sale is not complicated. The accomplice of the employee-fraudster pretends to buy merchandise, but the employee does not ring up the sale. The accomplice takes the merchandise without paying for it. To a casual observer, it will appear that the transaction is a normal sale. The employee bags the merchandise, and may act as though a transaction is being entered on the register, but in fact, the "sale" is not recorded. The accomplice may even pass a nominal amount of money to the employee to complete the illusion. A related scheme occurs when an employee sells merchandise to an accomplice at an unauthorized discount.

Employees also sometimes enlist accomplices to return goods that the employee has already stolen. This is an easy way for the employee to convert the stolen inventory into cash.

Asset Requisitions and Transfers

Asset requisitions and other documents that allow non-cash assets to be moved from one location in a company to another can be used to facilitate the theft of those assets. Employee’s use intrnal transfer paperwork to gain access to merchandise that they otherwise might not be able to handle without raising suspicion. These documents do not account for missing merchandise the way

false sales do, but they allow a person to move assets from one location to another. In the process of this movement, the thief steals the merchandise.

The most basic scheme occurs when an employee requisitions materials for some work- related project, then makes off with the materials. In some cases the employee simply overstates the amount of supplies or equipment it will take to complete his work and pilfers the excess. In more ambitious schemes the employee might invent a completely fictitious project that necessitates the use of certain assets he intends to steal.

EXAMPLE

An employee of a telecommunications company used false project documents to request approximately $100,000 worth of computer chips, allegedly to upgrade company computers. Knowing that this type of requisition required verbal authorization from another source, the employee set up an elaborate phone scheme to get the "project" approved. The fraudster used his knowledge of the company's phone. When the confirmation call was made, it was the perpetrator who answered the phone and authorized the project.

Dishonest employees sometimes falsify asset transfer forms so they can remove inventory from a warehouse or stockroom. The false documents allow the employee to remove merchandise from the warehouse, but instead of using it for a work-related purpose, the perpetrator simply takes it home. The obvious problem with this type of scheme is that the person who orders the merchandise will usually be the primary suspect when it turns up m1sstng.

EXAMPLE A manager requested merchandise from the company warehouse to be displayed on a showroom floor: The pieces he requested never made it to the showroom, because he loaded them into a pickup and took them home. In some instances he actually took the items in broad daylight and with the help of another employee. This individual thought he was immune from detection because the merchandise was requested via computer using a management level security code. The code was not specific to any one manager, so there would be no way Of knowing which manager had ordered the merchandise. Unfortunately for the thief, the company was able to record the computer terminal from which the request originated The manager had used his own computer to make the request, which led to his undoing.

Purchasing and Receiving Schemes

Dishonest employees can also manipulate the purchasing and receiving functions of a company to facilitate the theft of inventory and other assets. It might seem that any purchasing scheme should fall under the heading of false billings, which were discussed earlier. There is, however, a distinction between the purchasing schemes that are classified as false billings and those that are classified as non-cash misappropriations.

If an employee causes his company to purchase merchandise that the company does not need, this is a false billing scheme. The harm to the company comes in paying for assets for which it has no use. On the other hand, if the assets were intentionally purchased by the company and later misappropriated by the perpetrator, this is classified as an inventory larceny scheme. Here the company loses both the value of the merchandise and the use of the merchandise.

Falsifyiing Incoming Shipments

One of the most common examples of an employee abusing the purchasing and receiving functions occurs when a person charged with receiving goods on behalf of the victim company-such as a warehouse supervisor or receiving clerk-falsifies the records of incoming shipments. If, for example, 1,000 units of a particular item are received, the perpetrator indicates that only 900 were received. By marking the shipment short, the perpetrator can steal the 100 units that are unaccounted for.

The obvious problem with this kind of scheme is the fact that the receiving report does not match the vendor's invoice, which will likely cause a problem with patent. In the example above, if the vendor bills for 1,000 units but the accounts payable voucher only shows receipt of 900 units of merchandise, then someone will have to explain where the extra 100 units went.

Some employees avoid this problem by altering only one copy of the receiving report. The copy that is sent to accounts payable indicates receipt of a full shipment so the vendor will be paid without any questions. The copy used for inventory records indicates a short shipment so that the assets on hand will equal the assets in the perpetual inventory.

Instead of marking shipments short, the perpetrator might reject portions of a shipment as not being up to quality specifications. The perpetrator then keeps the ~'substandard" merchandise rather than sending it back to the supplier. The result is the same as if the shipment had been marked short.

False Shipments of Inventory and Other Assets

To conceal thefts of inventory and other assets, employees sometimes create false shipping documents and false sales documents to make it appear that the inventory they take was sold rather than stolen. (See "False Shipments of Inventory and Other Assets" £1owchart.) The document that tells the shipping department to release inventory for delivery is usually the packing slip. By creating a false packing slip, a corrupt employee can cause inventory to be fraudulently delivered to himself or an accomplice. The "sales" reflected in the packing slips are typically n: ladeto a fictitious person, a fictitious company, or an accomplice of the perpetrator..

One benefit of using false shipping documents to misappropriate inventory or other assets is that the product is removed from the warehouse or Storeroom by someone other than the perpetrator. The victim organisation unknowingly delivers the targeted assets to the perpetrator of the scheme.

False packing slips allow inventory to be shipped from the victim company to the perpetrator, but alone they do not conceal the fact that inventory has been misappropriated. In order to hide the theft, fraudsters may create a false sale on the books so it appears that the missing inventory was shipped to a customer. Depending on how the victim organisation operates, the perpetrator may have to create a false purchase order from the "buyer," a false sales order,and a false invoice along with the packing slip to create the of a sale.

The result is that a fake receivable account goes into the books for the price of the misappropriated inventory. Obviously, the "buyer" of the merchandise will never pay for it. How do employees deal with these fake receivables? In some cases, the employee simply lets the receivable age on his company's books until it is eventually written off as uncollectible. In other instances he might take affirmative steps to remove the sale-and the delinquent receivable that resets-from the books.

EXAMPLE

An employee generated false invoices and delivered/hem 10 the company warehouse for shipping. The invoices were then marked "delivered" and sent to the sales office. The perpetrator removed all copies of the invoices from the files before they were billed 10 the fictitious custome1:

Another common way to get rid of delinquent receivables that result from theft schemes is to write off the receivables to accounts such as discounts and allowances, bad debt expense, orJost and stolen assets.

Instead of creating completely fictitious sales, some employees understate legitimate sales so that an accomplice is billed for less than delivered. The result is that a portion of the merchandise is sold at no cost.. In atypical scenario, a salesman fills out shipping tickets, which are forwarded to the warehouse. After the merchandise is shipped, the salesman instructs the warehouse employees to return the shipping tickets to him for "extra work" before they are sent to the invoicing department; The salesman then alters the shipping tickets, reducing either the quantity of merchandise sold or the price per unit sold.

Write-offs are often used to conceal the theft of assets after they have been stolen. In some cases, however, assets are written off in order to make them available for theft. For instance, an employee with the authority to declare inventory obsolete can write off this inventory as "scrap." Once assets are designated as scrap, it is often easier to misappropriate them. Fraudsters may be allowed to take the "useless" assets for themselves, buy them or sell them to an accomplice at a greedy reduced price, or simply have the assets away.

Concealing Inventory Shrinkage

When inventory is stolen, the key concealment issue for the perpetrator is shrinkage. Inventory shrinkage is the unaccounted-for reduction in the company’s inventories those results from theft. For instance, assume a computer retailer has 1,000 computers in stock. After working day, an employee loads 10 computers into a truck and takes them home. Now the company only has 990 computers, but since there is no record that the employee took 10 computers, the inventory

records still show 1,000 units on hand. The company has experienced inventory shrinkage in the amount of 10 computers.

Shrinkage is one of the red flags that signal fraud. The goal of the perpetrator is to proceed with his scheme undetected, so it is in his best interest to prevent anyone from looking for missing assets. This means concealing the shrinkage that occurs from asset theft.

Inventory and other assets are typically tracked through a two-step process. The first step, the perpetual inventory, is a running count that records how much inventory should be on hand. When new shipments of merchandise are received, for instance, this merchandise is entered into the perpetual inventory. Similarly, when goods are sold they are removed from the perpetual inventory records. In this way a company tracks its inventory on a day-to-day basis.

Periodically, a physical count of assets on hand should be made. In this process, someone actually goes through the storeroom or warehouse and counts everything that the company has in stock. This total is then matched to the amount of assets reflected in the perpetual inventory. A variation between the physical inventory and the perpetual inventory totals is shrinkage. While a certain amount of shrinkage may be expected in any business, large shrinkage totals may indicate fraud.

Altered Inventory Records

One of the simplest methods for concealing shrinkage is to change the perpetual inventory record so that it will match the physical inventory count this is also known as a forced reconciliation of the account. The perpetrator simply changes the numbers in the perpetual inventory to make them match the amount of inventory on hand, For example, the employee might credit the perpetual inventory and debit the cost of sales account to bring the perpetual inventory numbers into line with the actual inventory count. Instead of using correcting entries to adjust the perpetual inventory, some employees simply delete "or cover up the correct totals and enter new: numbers.

There are two sides to the inventory equation: the perpetual inventory and the physical inventory. Instead of altering the perpetual inventory, a perpetrator who has access to the records from a

physical inventory count can change those records to match the perpetual inventory. Returning to the computer store example, assume the company counts its inventory every month and matches it to the perpetual inventory. The physical count should come to 990 computers, since that is what is actually on hand; If the perpetrator is someone charged with counting inventory, he can simply write down that there are 1,000 units on hand.

Factious Sales and Accounts Receivable

When the perpetrator makes an adjusting entry to the perpetual inventory and cost of sales accounts as discussed above, there is no sales transaction on the books that corresponds to these entries. In order to fix this problem, a perpetrator might enter a debit to accounts receivable and a corresponding credit to the sales account so that it appears the missing goods have been sold.

Of course, the problem of payment then arises, because no one is going to pay for the goods that were "sold"in this transaction. There are two routes that a fraudster might take in this circumstance. The first is to charge the sale to an existing account. In some cases, employees charge fake sales to existing receivables that are so large that the addition of the assets that the perpetrator has stolen will not be noticed. Other corrupt employees charge the "sales" to accounts that are already aging and will soon be written off. When these accounts are removed from the books, the perpetrator's stolen inventory effectively disappears. The other adjustment that is typically made is a write-off to discounts and allowances.

Write-Off of Inventory and Other Assets

Writing off inventory and other assets is a relatively common way for employees to remove assets from the books before or after they are stolen. This eliminates the problem of shrinkage that inherently exists in every case of non-cash asset misappropriation.

Physical Padding

Most methods of concealment deal with altering inventory records, either changing the perpetual inventory or miscounting during the physical inventory. In the alternative, some employees try to make it appear that there are more assets present in the warehouse or stockroom than there

actually are. Empty boxes, for example, may be stocked on shelves to create the illusion of extra inventory.

Detection of Inventory Schemes Statistical Sampling

Companies with inventory accounts typically have enormous populations of source documents. Statistical sampling allows the fraud examiner to inspect key attributes on a smaller portion (or sample) of those documents. For example, the examiner may select a statistically valid, random sample of purchase requisitions to determine that all requisitions in the sample selected were properly approved. Statistical sampling enables the examiner to predict the occurrence rate for the population and, therefore, .determine with some accuracy the error rate or the potential for fraud.

Other items that may be sampled on a statistical basis include the following: .Receiving reports

.Perpetual inventory records .Raw materials requisitions .Shipping documents .Job cost sheets

The attributes tested for on the above mentioned documents might include a specific date, item, or location.

Perpetual Inventory Records

Unexplained entries in the perpetual records might reveal embezzlement losses.

.Are all the reductions to the perpetual inventory records explained by source documents (such as sales invoices, approvals to remove to scrap inventory, or spoilage)?

.Are all increases in perpetual records explained by source documents such as receiving reports?

Shipping Documents

Inventory theft may be uncovered by answers to questions such as: .Are all sales properly matched with a shipping document? .Are any shipping documents not associated with a sale? .Is inventory disappearing from storage?

Physical Inventory Counts

Physical inventory counts can sometimes give rise to inventory theft detection. However, because other explanations satisfy inventory shortages, historical analysis of inventory is usually necessary. Furthermore, if the only metho4 used to detect inventory fraud is the year-end physical count, the perpetrators will have had to devise concealment methods to circumvent potential detection;

Analytical Review

By using an analytical review, inventory fraud may be detected because certain trends become immediately clear. For example, if the cost of goods sold increases by a disproportionate amount relative to sales, and no changes occur in the purchase prices, quantities purchased, or quality of products purchased, the cause of the disproportionate increase in cost of goods sold might be one of two things: (1) ending inventory has been depleted by theft, or (2) someone has been embezzling money through a false billing scheme (i.e., submitting invoices and collecting the payments for inventory that was never delivered).

An analytical review of all the component parts of the cost of goods sold should indicate to the examiner where to direct further inquiries. For example, assuming that the type of inventory purchased is the same and there is no change in the manufacturing process or purchase price, Sales and cost of sales change from $5,650,987 and $2,542,944 to $6,166,085 and $2,981,880, respectively, what is the data telling the examiner? To be~, sales have increased by 9.12 percent whereas cost of sales increased by 17.26 percent. The profit mar~ has decreased by3 percent (from 55 to 52 percent). Based on this data, the fraud examiner might want to look further at the components of inventory, such as beginning inventory, purchases, and ending inventory. If beginning inventory was $1,207,898, purchases were $2,606,518, and $2,604,972; respectively and ending inventory was $894,564, then an inventory matrix would look like the following:

Inventory purchases, as a percentage of sales, have declined from 46.13% to 42.25 percent. From this example, one can hypothesize that: (1) inventory purchases were purposely increased in year one only to be liquidated in year two, (2) the increased sales in year two were unexpected and the purchase of inventory did not keep pace with the sales, or (3) there might be some fraud scheme

in inventory. If, by interview, the examiner is unable to ascertain a reasonable explanation such as (1) or (2) above, then further examination of the ending inventory may be warranted.

The fraud examiner may next look at the differences in the physical inventory procedures, to see if that created a more (or less) accurate inventory count at the end of either year one or year two. If there is no other logical explanation, then further investigation into these and other inventory accounts may be necessary to explain the anomalies occurring in inventory.

Computer-Generated Trend Analysis

The computer can be used to facilitate obtaining lists of items with specified attributes. For example, in a lumberyard operation, the computer can be programmed to list all purchases

of four by four cedar fence posts eight feet in length. Examine all the source documents that are represented by the listing. By examining the source documents for each of these purchases, the examiner can plot trends to determine the occurrence of the following (or other) patterns:

Fraud Audit Report

Question No 36. How does a "Fraud Audit report" look a like? This post provides an example of a fraud audit report. The allegation is that a company manager perpetrated a false billing scheme using a front company.

Ans:

I. Background and Assumptions

Scott Graham, Esq., counsel for Prudent Auditing Corp. in the matter of The XYZ Company has engaged Lie Dharma Putra, CPA and CFE, to examine the Prudent Auditing Corp.'s documents and records for the direct purpose of offering opinions regarding the payments to The XYZ Company.

I have prepared this report summarizing the opinions I have formulated from reviewing documents on July 24, 2010. The documents were made available to me via the controller of Prudent Auditing Corp. I am qualified to issue such opinions based on my education, training, experience, and accreditations in such matters.

II. Statement of Opinions

My opinions are based on an independent examination of relevant materials provided by the controller and legal counsel of the Prudent Auditing Corp., independent research and investigation, authoritative treatises, and my past experience and professional knowledge in matters of this nature. The opinions contained in this report are as of October 31, 2010.

Insofar as discovery is continued in this matter, I reserve the right to supplement or otherwise amend this report regarding factual assumptions, theories of fraud, and statements of opinions.

1. Credible evidence exists to suggest that the XYZ Company is a front company.

2. Credible evidence exists to suggest that the services described on the XYZ invoices were not provided to the Prudent Auditing Corp.

3. Credible evidence exists to suggest that internal employees either conspired to commit or committed the possible misappropriation of funds.

4. Credible evidence exists to suggest that person(s) involved knowingly converted Prudent Auditing Corp. funds for their own personal benefit.

5. Credible evidence exists to suggest that the Prudent Auditing Corp. has suffered a loss of $ 120,000.

The reasons, causes, and motives for these occurrences can be resolved with a thorough and complete investigation of the XYZ Company's financial records and the personal financial records of identified internal employees.

III. Relevant Information

I have relied on the preceding facts and information to formulate my opinion contained in this report.

1. The XYZ Company invoices, the supporting purchase orders, and purchase requisitions.

2. The Prudent Auditing Corp. general ledger and cash disbursement ledger for the 20X6 and 2010 calendar year.

3. Copies of the front and back of Prudent Auditing Corp. canceled checks issued to the XYZ Company.

4. Prudent Auditing Corp. personnel files.

5. Prudent Auditing Corp. purchasing and disbursement polices and procedures.

6. Interviews of Prudent Auditing Corp. employees.

IV. Exhibits

Exhibit 1: Listing of payments to The XYZ Company

Exhibit 2: Copies of XYZ Company invoices

Exhibit 3: Copies, front and back, of Prudent Auditing Corp. canceled checks payable to The XYZ Company

V. Factual Background and Assumptions

1. Credible evidence exists to suggest that The XYZ Company is a front company.

(a). The XYZ Company billing head indicates a mailing address of PO Box 934.

(b). The accounts payable function has no record of the physical address of The XYZ Company.

(c). The telephone number listed on the invoice was answered by an answering service on three different occasions over a ten – day period. The XYZ Company has not returned our messages.

(d). The manager who purported to engage The XYZ Company was not aware of the physical location of The XYZ Company.

(e). The incorporating documents for The XYZ Company were filed by the XYZ Formation Company.

(f). The Prudent Auditing Corp. checks were endorsed with a stamp that states "for deposit in Account Number 06041977".

2. Credible evidence exists to suggest that the services described on the XYZ invoices were not provided.

(a). The XYZ Company provided no reports detailing the work performed under its consulting agreement.

(b). The agreement between the Fraud Audit Corp. and The XYZ Company is silent on providing a report summarizing results or recommendations.

(c). The Prudent Auditing Corp. manager who retained The XYZ Company indicated that all meetings with The XYZ Company occurred at the Prudent Auditing Corp offices.

(d). The Fraud Audit Corp. manager was unable to provide a list of other Prudent Auditing Corp. employees who were present at the meetings with The XYZ Company.

(e). There were no entries on the Fraud Audit Corp. manager's calendar indicating meetings with The XYZ Company.

(f). We were unable to identify any Fraud Audit Corp. employees who had a recollection of meeting with The XYZ Company.

(g). The XYZ Company invoices ' description of services stated "Services Rendered".

3. Credible evidence exists to suggest that internal employees either conspired to commit or committed the misappropriation of funds.

(a). The hiring manager has stated he has no specific recollection of approving The XYZ Company invoices.

(b). The approval signature purported to be that of the Fraud Audit Corp. ' s manager is similar to other known writing samples of the Fraud Audit Corp. ' s manager.

(c). The accounts payable function has no specific recollection of processing The XYZ Company invoices for payment.

(d). The first payment date on the Prudent Auditing Corp.'s canceled check to The XYZ Company occurred five days after the incorporation of the date of The XYZ Company.

(e). The incorporation data was obtained from the Secretary of State's Web site.

4. Credible evidence exists to suggest that person(s) involved knowingly converted Prudent Auditing Corp. funds for their own personal benefit.

(a). The Fraud Audit Corp. manager is unable to provide any evidence that the services described on the vendor invoices were provided.

(b). The XYZ Company is unwilling to respond to our inquiries regarding the investigation.

5. Credible evidence exists to suggest that the Prudent Auditing Corp. has suffered a loss of $ 120,000.

(a). As identified on Exhibit 1, there are 12 payments to The XYZ Company totaling $ 120,000.

(b). Each payment was for $ 10,000.

VI. Documents Necessary to Determine that the XYZ Company Is a Front Company

1. Documents submitted to the formation company to create the corporation.

2. Application for Creation of a Corporation used by the formation company to create The XYZ Company.

3. Documents submitted to the formation company for payment of services rendered to The XYZ Company.

4. The formation company telephone records for the month of creation and the month before and after the creation.

VII. Documents Necessary to Determine that Services Described on The XYZ Invoices Were Not Provided to the Prudent Auditing Corp.

1. No additional documents are required.

2. A formal statement from the Prudent Auditing Corp. manager ' s recollection of the business relationship with The XYZ Company.

VIII. Documents Necessary to Determine that Internal Employees Either Conspired to Commit or Committed the Misappropriation of Funds

1. No additional documents are required.

2. A handwriting expert should be considered to establish the authenticity of the approval signature on The XYZ Company ' s invoices.

IX. Documents Necessary to Determine that Prudent Auditing Corp. has Suffered a Loss of $ 120,000

1. No additional records are required.

X. Documents Necessary to Determine that Person(s) Involved Knowingly Converted Prudent Auditing Corp. Funds for Their Own Personal Benefit

1. All XYZ Company bank records of any and all accounts under signature authority of any of the named parties or entities, including but not limited to the known account numbers.

2. All personal bank records of any and all accounts under signature authority of any of the named parties or entities, including but not limited to the known account numbers.

3. All open or closed checking, savings, and money market accounts.

(a). Account opening documents including signature cards, copies of identification documents provided, and, if business account, copy of corporate resolution to open account and other business documents provided, which may include articles of incorporation for the business.

(b). Bank statements.

(c). Canceled checks (both sides).

(d). Deposit tickets and items (both sides of items, including ATM anddirect deposits).

(e). ATM withdrawals.

(f). Credit and debit memos.

(g). Telephone transfer slips.

(h). Wire transfer records.

(i). Forms 1099 or backup withholding statements.

XI. Document Request General Counsel of the Prudent Auditing

Corporation has been requested to obtain the documents requested in this report. The bank providing the bank records of The XYZ Company should provide a certification letter as to the authenticity of the bank records.

The examination of the requested documents could result in a further request for documents for an expanded period of time, either greater than the document request date or a more historical time frame.

XII. Compensation

I am being compensated for my services in this matter at my firm's standard hourly rates for my work in analyzing the defendant's data and underlying documentation and for preparing this report.

XIII. Professional Background

My CV has been provided to the General Counsel of the Prudent Auditing Corp.

XIV. End of Report

Insofar as discovery is continued in this matter, I reserve the right to supplement or otherwise amend this report regarding factual assumptions, theories of fraud, and statements of opinions.

Respectfully submitted,

Lie Dharma Putra, CPA & CFE

Question No 37. Sample report for Fraud Examination.

Ans:

SAMPLE FRAUD EXAMINATION REPORT

TO: [NAME] **HAL B. MARLOW**
[TITLE] **CHIEF EXECUTIVE OFFICER**

FROM: [NAME] **LOREN D. BRIDGES**
[TITLE] **CERTIFIED FRAUD EXAMINER**

RE: [SUBJECT LINE] **EXAMINATION OF POTENTIAL ASSET MISAPPROPRIATION**

DATE: [REPORT DATE] **MAY 23, 2009**

I. Background

[The background section should generally be about two paragraphs. It should state very succinctly why the fraud examination was conducted (e.g., an anonymous tip was received, an anomaly was discovered during an audit, money or property was missing).

You may also state who called for the examination and who assembled the examination team.]

On January 28, 2009, the fraud examination unit at Bailey Books received an anonymous telephone call on its fraud hotline from an unidentified man who claimed that he was a former supplier to Bailey. The caller alleged certain improprieties in the bidding and procurement process.

Based upon this initial predication, a fraud examination was conducted, which included reviews of relevant records and interviews of appropriate personnel.

II. Executive Summary

[For a simple fraud examination, the executive summary should be no more than four or five paragraphs. For a more complex case, the summary may reach a page in length.

In this section, you should also summarize what actions you performed during the fraud examination, such as reviewing documents, interviewing witnesses, conducting analyses or tests, etc.

It provides the reader with an overview of what you did during the examination process.

At the end of this section, you should summarize the outcome of the examination. For example,

"$50,000 in checks was deposited into an account owned by Bob Wilson. When confronted with this information, Wilson stated that he had only borrowed the money and meant to pay it back."]

The fraud examination commenced when Loren D. Bridges, CFE, received a telephone call from an unidentified man who said that he had been a long-term supplier to Bailey for sundry office supplies and paper. The caller said that ever since Linda Reed Collins had taken over as Purchasing Manager, he had been gradually "squeezed out" from doing business with Bailey.

Linda Reed Collins has been employed in the purchasing department of Bailey Books since June 1, 2004. She was promoted to Purchasing Manager effective November 8, 2006.

The Fraud Examination Team reviewed selected purchases from 2006 to 2007 and conducted interviews of key participants and Bailey employees who we believed may have information regarding the misappropriation of assets. The Team reviewed purchasing guidelines, personnel files of interviewees, and various financial documents relating to both Bailey Books and Linda Reed Collins.

After obtaining sufficient documentation, the Team interviewed Linda Reed Collins, who gave a full signed confession to her misdeeds.

III. Scope

[This section should consist of just one paragraph explaining what the scope of the fraud examination was. For example, "Determine whether or not inventory was misappropriated from the warehouse," or "Determine why money is missing from the bank account."]

The objective of the Fraud Examination Team was as follows:

• Determine the existence of a possible misappropriation of assets of Bailey Books, Incorporated. The examination is predicated upon an anonymous telephone call alleging improprieties on the part of Linda Reed Collins, Bailey's purchasing manager

V. Approach

[This section gives a brief description of the following items:

• Fraud examination team members

• Procedures (generally what documents were reviewed or what tests were conducted)

• Individuals interviewed

It provides a handy reference as to who was involved in the fraud examination, what the team reviewed, what tests or analyses were conducted, and what individuals the team interviewed.]

Fraud Examination Team Members

Loren D. Bridges, CFE, Bailey Books; Tonya Vincent, CFE, Bailey Books

Procedures

As part of the examination of this matter, the Team took the following actions:

• Obtained, reviewed, and analyzed memoranda pertaining to the anonymous call described previously.

• Obtained, reviewed, and analyzed Bailey Books' financial documentation, including purchase records, invoices, and canceled checks.

• Obtained, reviewed, and analyzed records from the St. Augustine County Courthouse regarding civil actions in which Edward J. Collins and Linda Reed Collins were named; records from the Florida Secretary of State's Office regarding Collins Marine Corporation; records of chattel mortgages held by Linda Reed Collins and Edward J. Collins; financial records from Dun &

Bradstreet regarding Collins Marine Corporation; and public records regarding the financial condition of Linda Reed Collins and Edward J. Collins.

• Conducted surveillance activity in order to determine whether the two key individuals in the matter were involved in an illicit relationship.

Individuals Interviewed: The following individuals were interviewed in person by members of the Fraud

Examination Team:

• Mark W. Steinberg, CPA (Chief Financial Officer, Bailey Books)

• Roger Donald McGuire (Purchasing Agent, Bailey Books)

• Mary Rodriguez De La Garza (Purchasing Agent, Bailey Books)

• Sara Louise Dawson (Former Employee, Bailey Books)

• Thomas C. Green (Attorney, Sharp, Green and Langfrom, P.A.)

• Lincoln S. Wyzokowski (General Counsel, Bailey Books)

Becky Robinson (Accounts Payable Clerk, Bailey Books)

• Ernie Quincy (Warehouse Manager, Bailey Books)

• David Levey (Director of Sales, Jerrico International Paper Company)

• James R. Nagel (Sales Representative, Orion Corporation)

• Owen Stetford (Chief Financial Officer, Orion Corporation)

• Linda Reed Collins (Purchasing Manager, Bailey Books)

V. Findings

[This section contains the details of the fraud examination. It will generally consist of several pages.

In this section you should describe what tasks you performed and what you found. Provide enough detail so that the reader understands what occurred, but not so much detail that the reader begins to lose interest or becomes bogged down in the details. The reader wants to know how many invoices were forged, who was involved, how did they do it, what proof do you have, etc.

If the findings section is long, you may wish to use subheadings for particular topics or individuals to make it easier for the reader to stay organized.

The information can be presented either chronologically or by topic — whatever makes it easier for the reader to follow.]

Based on the documents reviewed, information collected, and interviews conducted during the course of the fraud examination, the Team finds as follows:

• Did the Fraud Examination Team determine the existence of a possible misappropriation of assets of Bailey Books Incorporated?

Yes. The documents and information reviewed and interviews conducted by the Fraud Examination

Team during the course of the examination indicate that Linda Reed Collins, together with James R. Nagel, did knowingly embezzle approximately $197,773 from Bailey Books over four years. During the fraud examination, the Team analyzed financial documents and conducted interviews to corroborate the statements of an anonymous caller. The following is a summary of the evidence and information supporting the Fraud Examination Team's findings:

On January 28, 2009, an anonymous call was received by the fraud hotline at Bailey Books,

Incorporated, from a former supplier to Bailey Books. The caller alleged that after Linda Reed

Collins took over as Purchasing Manager in 2006, she eliminated him as a supplier. A subsequent review of purchases made by Bailey Books from 2006 to 2008 showed that a continuously increasing share of the company's paper business was being given to Orion Corp., even though Orion submitted written bids in only 63 percent of the cases.

On February 1, 2009, Mark W. Steinberg, CFO of Bailey Books, Inc., was interviewed. The purpose of the interview was to inform him of the proposed fraud examination, obtain his approval, and secure information from him regarding the purchasing process at Bailey Books. In addition to summarizing his responsibilities regarding purchasing at Bailey Books, Mr. Steinberg stated that in

December 2006 he sent a memo to all the division heads at Bailey Books informing them that all purchases over $50,000 would from then on require at least three written bids.

We next examined the personnel records. A review of Linda Reed Collins's file showed only that she had been consistently rated "exceptional" by her supervisors in annual reviews.

On February 4, 2009, an interview was conducted with Roger Donald McGuire, Purchasing Agent at Bailey Books. After summarizing the purchasing process at Bailey Books, he stated that he had no knowledge of any improprieties committed by Ms. Collins.

The next interview conducted was with Mary Rodriguez De La Garza, a coworker of Ms. Collins's in the Purchasing Department at Bailey Books. During the interview Ms. De La Garza stated that, regarding the purchasing process, it is sometimes not practical to obtain bids, such as in emergency situations or when they are short on time. She went on to reveal that she had suspected Ms. Collins was having an affair with James R. Nagel, the salesman for Orion Corp. In addition, Ms. De La

Garza said she believed that Ms. Collins and her husband were having marital and financial problems. She also mentioned that Sara Louise Dawson, a former employee under Ms. Collins, had left on bad terms.

The next interview was with Sara Louise Dawson, who wanted to consult with her attorney before making an official statement. Ms. Dawson's attorney, Thomas C. Green, later contacted the Fraud Examination Team to let them know that Ms. Dawson was interested in making a statement, but only in exchange for an indemnity against all claims arising out of her cooperation. After meeting with Mark Steinberg and Lincoln S. Wyzokowski, General Counsel at Bailey Books, Ms. Dawson's and Mr. Green's proposal was accepted

On March 3, 2009, Ms. Dawson made her statement, which included the following:

• After Ms. Collins was promoted to Purchasing Manager, she began favoring Orion Corp. for paper purchases.

• On two occasions in 2008, Ms. Collins authorized prepayment on substantial purchases from Orion, even though Ms. Dawson had complained about Orion's poor quality and service. Later Ms. Dawson found out that the orders were never received.

• Other vendors had complained of being squeezed out of business with Bailey Books after

Ms. Collins became manager.

Ms. Dawson referred the Team to Becky Robinson in Accounts Payable for further information about the orders. Ms. Robinson was interviewed and provided copies of the two prepaid invoices to Orion Corp., the amounts of which were $102,136 and $95,637. In addition, Ms. Robinson said that Ernie Quincy in Receiving would be able to verify if the two shipments had ever been received.

On April 8, 2009, Ernie Quincy, the Warehouse Manager at Bailey Books, was interviewed and verified that the two shipments in question were never received. The next day, copies of the two checks given to Orion Corp. for payment of the goods that were never received were examined.

An interview with David Levey from Jerrico International Paper Company yielded the following information:

• At the time Levey began at Jerrico, Bailey Books was a major customer of theirs, but since then their sales to Bailey had dwindled.

• Levey attempted to revive business with Bailey Books, but by then rumors were circulating about an inappropriate relationship between Mr. Nagel of Orion Corp. and Ms. Collins.

• According to Levey, Mr. Nagel had a "bad reputation" in the industry.

Ms. De La Garza phoned the Team on April 13, 2009, to let them know that Ms. Collins had plansto meet Mr. Nagel at the bar at the Hotel Atlantic that afternoon. The Team set up

surveillance of their meeting and reported that Ms. Collins and Mr. Nagel met at 5:55 p.m. and ordered drinks.

They held hands under the table, kissed, and left the bar at 7:02 p.m. to go to room 652.

A review of St. Augustine County records showed that Edward J. Collins (Ms. Collins's husband) was a defendant in three civil actions. The circumstances of the actions indicated that the Collinses were having financial troubles.

A review of the Florida Secretary of State's records showed that the Collinses were the incorporators of Collins Marine Corporation.

A review of UCC filings showed that the Collinses had three liens in their name.

A net-worth analysis was performed on the Collinses based on information assembled from public records. It showed unexplained income of $31,632.

In an April 19, 2009 interview, Mr. Nagel stated that his relationship with Ms. Collins was purely professional and denied any improprieties regarding Orion's business with Bailey Books. Mr. Nagel also refused to provide any of Orion's financial information pertaining to the two invoices in question.

On April 21, 2009, Owen Stetford, the CFO of Orion Corp., was interviewed and stated he was unable to provide any copies of actual financial information, but that Orion had no record of any receipt of payment for the invoices in question, nor any record that such orders had been placed or shipped. In addition, Mr. Stetford said that Orion had no corporate accounts at Florida Marine

National Bank, the bank at which the checks from Bailey Books were deposited. Mr. Stetford also stated that the correct corporate name is Orion Corporation, not Orion Paper Company, as the endorsements indicated.

On May 1, 2009, Mr. Nagel was again interviewed. After being confronted with questions and evidence regarding the two payments and the bank account to which they were deposited, Mr. Nagel voluntarily gave a statement attesting to his involvement with Ms. Collins in the embezzlement of funds from Bailey Books. He attested to the following:

• In 2008, Ms. Collins told Mr. Nagel that she would approve the payment of invoices to Orion Corp. for product that would not be delivered. Ms. Collins authorized the payment of two invoices in the amounts of $102,136 and $95,637, but no product was shipped on the invoices. Ms. Collins and Mr. Nagel established a bank account in the name of Orion Paper Company at Florida Marine National Bank and divided the proceeds of the invoices equally.

On May 1, 2009, Ms. Collins voluntarily gave a statement, which included the following:

• Ms. Collins stated that, starting in 2007, she accepted money from Mr. Nagel to ensure that

Orion Corp. received preferential treatment in supplying Bailey Books with stationery and paper products. On those occasions, she was aware that Bailey Books was not obtaining the best product at the lowest possible price from Orion; in other words, the price charged was substantially higher than market value.

• Ms. Collins stated that on two occasions in 2008, she authorized the payment of invoices for $102,136 and $95,637 without any receipt of merchandise.

• Ms. Collins estimated that she had received in excess of $150,000 in connection with Mr. Nagel.

VI. Summary

[This section should be one or two paragraphs and should succinctly summarize the results of the fraud examination. It should be similar to the outcome stated at the end of the Executive Summary section.]

This report reflects that Linda Reed Collins, a purchasing agent for Bailey Books, Inc., furnished a signed statement on May 1, 2009, indicating she had accepted at least $197,773 in commercial bribes and other illicit income in a conspiracy with James R. Nagel, an account representative for Orion Corporation, St. Augustine, Florida.

The statements made by Collins are corroborated by the documentary evidence and the interviews of other witnesses as described herein.

VII. Impact to Bailey Books

[This section should be one or two paragraphs and should succinctly summarize the results of the fraud examination. It should be similar to the outcome stated at the end of the Executive Summary section.]

Over the course of four years, Linda Reed Collins, in partnership with James R. Nagel, misappropriated an estimated $197,773 from Bailey Books, Incorporated.

Additional amounts were lost due to Bailey's overpaying for merchandise sold to it by Nagel. Those amounts have not been calculated.

VIII. Recommendations

[This section is optional. There may be instances where you wish to discuss remedial measures or specific recommendations in a separate document. If you do wish to include this section, you should state what follow-up action is necessary or recommended, including remedial measures such as a review of internal controls, introduction of a hotline, increased security, etc.]

It is the policy of Bailey Books to report such matters to the appropriate authorities and to assist in criminal prosecution. A full review of internal controls should be conducted to determine how such incidents can be detected in the future.

Fraud Investigation for the Auditor

Investigation implies an inquiry into the accounts and records of a business concern. It is an examination of accounts and records of an undertaking with some special purpose in view. The main purpose of such inquiry is to ascertain the true financial position of the business concern or its normal profit earning capacity or the extent of fraud, if any, or to inquire about the suspected mismanagement etc. So, the investigation is a sort of special audit with a particular job in view.

A) Investigation

B) Auditing

PURPOSE

A) The purpose of investigation varies from Business to business.

B) The purpose of audit is to determine the true and fair view.

RECORD

A) The investigation relates to critical checking of particular records.

B) The audit relates to checking of all the books and records of particular period.

OWNERS

A) The investigation may be conducted on behalf of owners and outsider like investors.

B) Audit is conducted on behalf of owners only & they make the appointment.

CHECKING

A) Investigation work can be complete thorough cent percent checking.

B) Audit work may be completing thorough test checking.

TIME

A) The investigation has no time limit. It may relate to many years.

B) The audit of accounts is made for a particular time period.

QUALIFICATION

A) The investigator may or may not be a Chartered accountant.

B) The auditor is usually a chartered accountant.

EMPLOYEES

A) The investigator may examine employees personally.

B) The auditor does not examine personally.

COMPULSORY

A) The investigator is voluntary. It may become compulsory in certain cases.

B) The audit work is compulsory under Law for companies and other concern.

SEQUENCE

A) The investigation is usually conducted after the audit of accounts.

B) The audit is usually conducted before investigation of accounts.

DISCLOSURE

A) There is no legal requirement to disclosed information in investigation.

B) The audit requires full disclosure of information under the law.

PRINCIPLES

A) The investigator is not bound, to follow accounting principles and policies.

B) The audit staff is bound to follow the accounting principles and policies.

ACCOUNTS

A) The investigation depends upon audited accounts for his work. Audited accounts Are not necessary for investigation.

B) The audit depends upon accounts for checking the business performance. Special audit may require audited accounts.

ADJUSTMENT

A) The investment can make necessary adjustment in the books of accounts.

B) The auditor cannot makes adjustment in the books of accounts.

EVIDENCE

A) The investigator collects substantive and conclusive evidence in support of his viewpoints.

B) The auditor collects prima facie evident to support his viewpoint.

CONTENTS

A) The investigator report is in detail. It can show documents examined, methods applied and whole work done.

B) The audit report is stereotype but conditional report may show more weakness of the business concern.

REGULAR

A) The investigation is not a regular feature of business. It is conducted occasionally.

B) The audit work is a regular matter. It is conducted every year.

RECOMMENDATION

A) The investigator can recommend the course any of action to overcome the weakness.

B) The auditor has no right to recommend course of action unless asked to do so.

SUSPICION

A) The investigation work is started with doubt. The investigator thinks that there is some thing wrong.

B) The audit work is started with out any suspicion. Auditors think that all matters are right.

REPORT

A) The investigation report is a personal document. It cannot be used as evidence.

B) The audit report is a legal document. It can be used as evidence.

Question No 38. Describe the sample organization policies in order to face the fraud in the organization.

Ans:

RESPONSIBILITIES FOR MANAGING THE RISK OF FRAUD - RISK OWNERSHIP

Accounting Officers

The Accounting Officer (AO) is personally accountable for his/her organisation and its risk management. A framework of senior level delegation is essential to ensure that the responsibility and authority for implementing control actions is clear. A mechanism for reporting to the AO on risk issues should be established. Managing fraud risks [internal and external fraud risks] is part of the management of all other risks and the same principles apply.

Senior Management

Overall responsibility for Managing the Risk of Fraud should be allocated to an appropriate senior officer, e.g. the Principle Finance Officer. Their specific responsibilities, which can be formally delegated, will depend to some extent with the level of fraud risk the organisation is exposed to but should include some or all of the following:

• Developing a fraud risk profile and undertaking an annual review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;

• Establishing an effective anti-fraud policy and fraud response plan, commensurate with the level of fraud risk identified in the fraud risk profile;

• Developing appropriate fraud targets – SDA and/or PSA;

• Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;

• Establishing appropriate mechanisms for:

o reporting fraud risk issues;

o reporting significant incidents of fraud to the AO;

o reporting to the Treasury in accordance with GA 2000 Chapter 5; and

o coordinating assurances about the effectiveness of anti-fraud policies to support the

Statement of Internal Control

• Liaising with the Risk Management Committee and/or Audit Committee as appropriate – where an organisation has a Risk Management Committee it may be appropriate forthe reports to go to the AO via that committee. It may also be helpful to ask the Audit Committee to regularly consider fraud risk management issues and significant instances of fraudulent activity;

• Making sure that all staff are aware of the organization's anti-fraud policy and know what their responsibilities are in relation to combating fraud;

• Developing skill and experience competency frameworks;

• Ensuring that appropriate anti-fraud training and development opportunities are available

to appropriate staff in order to meet the defined competency levels;

• Ensuring that vigorous and prompt investigations are carried out if fraud occurs;

• Taking appropriate legal and/or disciplinary action against perpetrators of fraud;

• Taking appropriate action to recover assets;

• Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Operational Managers

Outside of any more formal delegation of the above duties, all other levels of management are responsible for:

• Implementing and maintaining effective controls to prevent fraud commensurate with the fraud risk profile, and

• Ensuring compliance with anti-fraud policies and fraud response plan.

Individual members of staff

Individual members of staff have an important role to play in combating fraud. Their responsibilities include:

• Acting with propriety in the use of official resources and in the handling and use of corporate funds whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers;

• Reporting details immediately to their line manager or other avenue for reporting fraud (e.g. whistleblowing arrangements) if they suspect that fraud has been committed or see any suspicious acts or events.

Internal Audit

The role of internal audit is to deliver an opinion to the Accounting Officer on the whole of an organisation's risk management, control and governance. In relation to fraud this will include the examination of the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation actively promotes an anti-fraud culture.

Internal audit will therefore assist in the deterrence of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of an organisation's operations. Internal audit's main responsibility is to ensure that management has reviewed its risk exposures and identified the possibility of fraud as a business risk.

Management has the responsibility for conducting fraud investigations but internal audit may be asked to assist, and in some organisations may have had responsibility for conducting investigations delegated to them. Fraud investigation is an area that requires specialist knowledge and where internal audit has this responsibility they need to develop and maintain appropriate levels of expertise.

PROMOTING AN ANTI-FRAUD CULTURE

Introduction

Fraud prevention involves more than merely compiling anti-fraud policies. It also involves putting in place effective accounting and operational controls and the maintenance of an ethical environment that encourages staff at all levels to actively participate in protecting public money and property.

Creating an anti-fraud culture involves:

• Having a clear statement of ethical values;

• Establishing a clear anti-fraud policy and fraud response plan;

• Promoting staff awareness of fraud;

• Recruiting honest staff (checking references etc); and

• Maintaining good staff morale.

Code of Ethics

As stewards of public funds civil servants must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality or benefits of any kind from a third party that might be seen to compromise their integrity.

All personnel should be reminded that they are bound by a code of ethics which, unless issued separately, should be stated in the anti-fraud policy. The ethics policy will:

• Explain that staff must follow the organisation's rules without circumventing controls;

• Explain what external interests may give rise to conflicts of interest and require any possible conflicts of interest to be declared;

• Define the organisation's policy on receiving gifts from external parties;

• Explain why it is necessary to keep certain information about the organisation confidential;

• Require employees to report suspected fraud to a named individual or via a fraud hotline;

• State that breach of the policy will be treated as a disciplinary offence;

• Provide cross-references to the organisations anti-fraud policy and fraud response plan.

Question No 39. Write down a sample of Anti-Fraud Policy for any organization.

Ans:

A fraud policy statement should be simple, focused and easily understood. It's contents may vary from organisation to organisation but you should consider including references to the organisation's determination to:

• Take appropriate measures to deter fraud;

• Introduce/maintain necessary procedures to detect fraud;

• Investigate all instances of suspected fraud;

• Report all suspected fraud to the appropriate authorities;

• Assist the police in the investigation and prosecution of suspected fraudsters;

• Recover from fraudsters any assets wrongfully obtained;

• Encourage employees to report any suspicion of fraud.

Source: The Fraud Advisory Panel's report "Fighting Fraud – A Guide for Small and Medium sized Enterprises"

An example of an anti-fraud policy follows.

Introduction

The [Organisation name] requires all staff at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible. The Department will not accept

any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately. The Department is committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

What is Fraud?

No precise legal definition of fraud exists; many of the offences referred to as fraud are covered by the Theft Acts of 1968 and 1978. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

"Fraud" is usually used to describe depriving someone of something by deceit, which might either be straight theft, misuse of funds or other resources, or more complicated crimes like false accounting and the supply of false information. In legal terms, all of these activities are the same crime –theft.

Avenues for Reporting Fraud

The Department has in place avenues for reporting suspicions of fraud. Staff should report such suspicions to their line managers, to the department's internal audit (or specialist fraud unit), or to the hotline set up for the purpose. All matters will be dealt with in confidence and in strict accordance with the terms of the Public Interest Disclosure Act 1998. This statute protects the legitimate personal interests of staff. Vigorous and prompt investigations will be carried out into all cases of actual or suspected fraud discovered or reported.

Responsibilities

• The Accounting Officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives.

The system of internal control is designed to respond to and manage the whole range of risks that a department faces. The system of internal control is based on an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively. Managing fraud risk will be seen in the context of the management of this wider range of risks.

- ✓ Overall responsibility for managing the risk of fraud has been delegated to….. [e.g. the
- ✓ Principal Finance Officer (PFO)]. Their responsibilities include:
- ✓ Developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;
- ✓ Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the fraud risk profile;
- ✓ Developing appropriate fraud targets – SDA and/or PSA;
- ✓ Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;

Establishing appropriate mechanisms for:

- ✓ reporting fraud risk issues;
- ✓ reporting significant incidents of fraud to the AO;
- ✓ Coordinating assurances about the effectiveness of anti-fraud policies to support the Statement of Internal Control.
- ✓ Liaising with the Risk Management Committee and/or Audit Committee.

Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud;

Developing skill and experience competency frameworks;

- ✓ Ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency levels;

- ✓ Ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected;
- ✓ Taking appropriate legal and/or disciplinary action against perpetrators of fraud;
- ✓ Taking appropriate disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;
- ✓ Taking appropriate disciplinary action against staff who fail to report fraud;
- ✓ Taking appropriate action to recover assets;
- ✓ Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Operational managers are responsible for:

• Ensuring that an adequate system of internal control exists within their areas ofresponsibility and that controls operate effectively;

• Preventing and detecting fraud;

• Assessing the types of risk involved in the operations for which they are responsible;

• Reviewing and testing the control systems for which they are responsible regularly;

• Ensuring that controls are being complied with and their systems continue to operate effectively;

• Implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place.

Internal audit is responsible for:

• Delivering an opinion to the Accounting Officer on the adequacy of arrangements for managing the risk of fraud and ensuring that the department promotes an anti-fraud culture;

• Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of the department's operations;

• Ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk;

• Assisting management in conducting fraud investigations.

Every member of staff is responsible for:

• Acting with propriety in the use of official resources and the handling and use of public funds whether they are involved with cash or payments systems, receipts or dealing with suppliers;

• Conducting themselves in accordance with the seven principles of public life set out in the first report of the Nolan Committee "Standards in Public Life". They are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership;

• Being alert to the possibility that unusual events or transactions could be indicators of fraud;

• Reporting details immediately through the appropriate channel if they suspect that a fraud has been committed or see any suspicious acts or events;

• Cooperating fully with whoever is conducting internal checks or reviews or fraud investigations.

Fraud Response Plan

The department has a Fraud Response Plan that sets out how to report suspicions, how investigations will be conducted and concluded. This plan forms part of the department's anti-fraud policy.

Conclusion

The circumstances of individual frauds will vary. The department takes fraud very seriously. All cases of actual or suspected fraud will be vigorously and promptly investigated and appropriate action will be taken.

Question No 40. How fraud opportunities can be reduces. Provide a roadmap.

Ans:

Introduction

Managers must ensure that the opportunities for fraud are minimised. Separation of duties, effective procedures and checks should prevent or deter fraud from occurring. Opportunities to commit fraud may be reduced:

• By ensuring that a sound system of internal control proportional to risk has been established and that it is functioning as intended;

• Through the "fear factor" (i.e. the risk of being caught or the severity of the consequences);

• By changing attitudes to fraud;

• By making it too much effort to commit.

Internal Control

"Control" is any action, procedure or operation undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Control is a response to risk – it is intended to contain uncertainty of outcome.

Some frauds arise because of a system weakness such as a lack of proper control over e.g. placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be the result of carelessness in carrying out a check, or it may be that too much trust has been placed in one individual with no effective separation of duties. Frauds that result from collusion may be more difficult to detect and prevent as these types of fraud tend to operate within the normal control environment.

In designing control, it is important that the control put in place is proportional to the risk. In most cases it is normally sufficient to design control to give a reasonable assurance of confining loss within the risk appetite of the organisation. Every control action has an associated cost and it

is important that the control action offers value for money in relation to the risk that it is controlling.

Generally speaking the purpose of control is to contain risk to a reasonable level rather than to remove it entirely.

When risks and deficiencies in the level of control are identified it is necessary to choose the most appropriate type of controls within the above guidelines. In respect of fraud risks, prevention is almost always preferable to detection. Strong preventive controls should therefore be applied wherever possible.

The following range of controls should be considered always ensuring that a balance between identified risk and value for money is maintained:

Physical security: this is a preventive measure which controls or monitors access to assets, documentation or IT systems to ensure that there is no unauthorized use, loss or damage.

Assets can range from the computer terminal that sits on the desk to the cheques sent out to pay suppliers. As a general principle all assets should be held securely and access to them restricted as appropriate. The control should apply not only to the premises but also to computers, databases, banking facilities, documents and any other area that is critical to the operation of the individual organisation. It may even be appropriate to restrict knowledge of the existence of some assets.

Access to computer systems is an important area that should be very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the data - the Data Protection Act requires computer and data owners to secure information held on their systems which concerns third parties. The threat to computers can come from both inside and outside an organisation. This threat may increase with the introduction of systems to meet the e-Government target (e.g. to allow the public to do business electronically with government departments, to link public sector computer systems etc). Computers are also vulnerable to theft, both in terms of hardware and software.

This type of theft has the additional cost of potential major disruption to the core operations of an organisation.

Organising: organising involves the allocation of responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner. Major principles in organizing relevant to fraud are:

• Clear definition of the responsibilities of individuals for resources, activities, objectives and targets. This includes defining levels of authority. This is a preventive measure which sets a limit on the amounts which may be authorised by individual officers. To be effective, checks need to be made to ensure that transactions have been properly authorised;

• Establishing clear reporting lines and the most effective spans of command to allow adequate supervision;

• Separating duties to avoid conflicts of interest or opportunities for abuse. This is also largely a preventive measure which ensures that the key functions and controls over a process are not all carried out by the same member of staff (e.g. ordering goods should be kept separate from receipt of goods); similarly authorization and payment of invoices; and

• Avoiding undue reliance on any one individual.

Supervision and checking of outputs: supervision is the function by which managers scrutinize the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. These act as both preventive and detective measures and involve monitoring the working methods and outputs of staff. These controls are vital where staff are dealing with cash or accounting records. Random spot checks by managers can be an effective anti-fraud measure.

Audit trail: this is largely a detective control, although its presence may have a deterrent effect and thus prevent a fraud. An audit trail enables all transactions to be traced through a system from start to finish. In addition to allowing detection of fraud it enables the controls to be reviewed.

Monitoring: Management information should include measures and indicators of performance I respect of efficiency, effectiveness, economy and quality of service. Effective monitoring, including random checks, should deter and detect some types of fraudulent activity.

Evaluation: policies and activities should be evaluated periodically for economy, efficiency and effectiveness. The management of the operation may perform evaluations, but they are usually more effective when performed by an independent team. Such evaluations may reveal fraud.

Staffing: Adequate staffing is essential for a system to function effectively. Weaknesses in staffing can negate the effect of other controls. Posts involving control of particularly high value assets or resources may need the application of additional vetting procedures. Rotation of staff between posts can help prevent or detect collusion or fraud.

Asset accounting: asset registers used for management accounting purposes can help detect losses that may be caused by fraud.

Budgetary and other financial controls: use of budgets and delegated limits for some categories of expenditure and other accounting controls should ensure that expenditure is properly approved and accounted for by the responsible manager. This should limit the scope for fraud and may result in some types of fraud being detected.

Systems development: controls over the development of new systems and modifications to existing systems or procedures are essential to ensure that the effect of change is properly assessed at an early stage and before implementation. Fraud risks should be identified as part of this process and the necessary improvements in control introduced.

The "Fear Factor": Major deterrents to perpetrating fraud are the risk of being caught and the severity of the consequences. The most important fact about deterrence is that it derives from perceived risk and not actual risk. A department may manage to increase the actual risk of detection but it will only achieve a deterrent effect if it ensures that perceptions of risk change too. Ways in which departments can do this include:

• Warnings on forms such as: "false statements may lead to prosecution";

• General publicity;

• Increasing the severity of penalties;

• Always taking appropriate action against known perpetrators of fraud.

Changing Attitudes to Fraud

The most effective strategies designed to change attitudes rely on motivation rather than fear. They aim to persuade people of the undesirability of a particular behaviour. Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect so it is important that departments carry out a full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns. Departments need to be clear about the objectives and targets of their campaigns.

Question No 41. How to develop an Anti-Fraud Program. Also discuss the typical types of Fraud and Fraud Tests.

Ans:

Seven Steps to Jump Start Your Anti-Fraud Program

Fraud whether it occurs in the form of carefully crafted Ponzi schemes, fudging financial reports or theft from one's own employer, is reaching alarming proportions and is not without its costs. Businesses and government agencies worldwide suffer hundreds of billions in lost or misused funds, diminished value, and irreversible damage to company reputation and customer trust.

Consider the alarming stats from the 2010 Report to the Nations on Occupational Fraud and Abuse from the Association of Certified Fraud Examiners (ACFE). According to the study, organizations worldwide lose an average of 5% of revenues to fraud each year for an average of $160,000.

Making matters worse (and no thanks to the economic downturn), many organizations have been forced to cut staff, freeze spending and skimp on internal controls and process assurance, which has left organizations more vulnerable to risk and fraud.

Now is the time for Internal Audit teams to step up fraud prevention and detection measures. Here is a quick list of priorities to kick start your program.

1. Build a profile of potential frauds

Take a top-down approach to your risk assessment, listing the areas in which fraud is likely to occur in your business and the types of fraud that are possible in those areas. Then qualify the risk based on the overall exposure to the organization. Focus on risks that have the greatest chance of reducing shareholder value.

2. Test transactional data for possible indicators of fraud

You must test 100% of the data, not just random samples. Fraudulent transactions, by nature, do not occur randomly. Transactions may fall within boundaries of certain standard testing and not be flagged.

3. Improve controls by implementing continuous auditing and monitoring

Strengthen controls over transaction authorizations and use continuous auditing and monitoring to test and validate the effectiveness of your controls. This method can drastically improve the overall efficiency, consistency and quality of your fraud detection processes

4. Communicate the monitoring activity throughout the organization

A big part of fraud prevention is communicating the program across the organization. If everyone knows there are systems in place that alert to potential fraud or breach of controls, and that every single transaction running through your systems is monitored, you've got a great preventative measure.

5. Provide management with immediate notification when things are going wrong

It is better to raise any issues right away than explain why they occurred later. Create audit reports with recommendations on how to tighten controls or change processes to reduce the likelihood of recurrence. And, don't forget to quantify the impact to the business.

6. Fix any broken controls immediately

Segregation of duties is important. If you can initiate a transaction, approve the transaction, and also be the receiver of the goods from the transaction, there is a problem.

7. Expand the scope and repeat.

Re-evaluate your fraud profile, taking into account both the most common fraud schemes and those that relate specifically to the risks that are unique to your organization, and move your investigative lens.

Typical Types of Fraud and Fraud Tests

Knowing what to look for is critical in building a fraud detection program. The following examples are based on descriptions of various types of fraud and the tests used to discover the fraud as found in Fraud Detection: Using Data Analysis Techniques to Detect Fraud.

Type of Fraud	Tests Used to Discover This Fraud
Fictitious vendors	➢ Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers ➢ Be alert for vendors with similar sounding names or more than one vendor with the same address and phone number
Altered invoices	➢ Search for duplicates ➢ Check for invoice amounts not matching contracts or purchase order amounts
Fixed bidding	➢ Summarize contract amount by vendor and compare vendor summaries for »»several years to determine if a single vendor is winning most bids ➢ Calculate days between close for bids and contract submission date by vendor »»to see if the last bidder consistently wins the contract
Goods not received	➢ Search for purchase quantities that do not agree with contract quantities ➢ Check if inventory levels are changing appropriate to supposed delivery of goods
Duplicate invoices	➢ Review for duplicate invoice numbers, duplicate date, and invoice amounts
Inflated prices	➢ Compare prices across vendors to see if prices from a particular vendor are »»unreasonably high
Excess quantities purchased	➢ Review for unexplained increases in inventory ➢ Determine if purchase quantities of raw materials are appropriate for production level ➢ Check to see if increases in quantities ordered compare similarly to previous contracts or years or when compared to other plants
Duplicate payments	➢ Search for identical invoice numbers and payments amounts ➢ Check for repeated requests for refunds for invoices paid twice
Carbon copies	➢ Search for duplicates within all company checks cashed; conduct a second search for gaps in check numbers

Duplicate serial numbers	➢ Determine if high value equipment a company already owns is being repurchased by checking serial numbers for duplicates and involvement of same personnel in purchasing and shipping processes
Payroll fraud	➢ Find out if a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck and extract all pay transactions for departure date less than date of current pay period
Accounts payable	➢ Reveal transactions not matching contract amounts by linking Accounts Payable files to contract and inventory files and examining contract date, price, ordered quantity, inventory receipt quantity, invoice quantity, and payment amount by contract

APPLYING TECHNOLOGY TO COMBAT FRAUD DATA FORENSICS: PEOPLE LIE, EVIDENCE DOESN'T

The Digital Workplace

- Contracts
- Projects
- Presentations
- Proposals
- Research documents
- E-mails
- Client lists
- Internet browsing
- News
- Entertainment

Data Forensics

Data forensics and high profile legal matters:

- Verizon
- Enron
- Martha Stewart

 Merck

Digital evidence has become commonplace in both criminal and civil matters.

The New Face of Crime

• Traditional "criminals" are easy to spot.

• Computer crime and abuse typically go unnoticed until the damage has been done.

Forensic Science Defined

Traditional physical evidence and electronic evidence:

"The methodical process of gathering, preserving, and analyzing evidence used to support a position in a court of law."

Risk of Internal Data Investigations

Risks associated with the collection of evidence and investigation by internal IT department staff:

 Considered a biased party

 Improper chain of custody

 Not trained

 In investigations

 Tools are not certified

 High risks of spoliation

 Not a credible expert

Where is Electronic Evidence?

• Servers

• Laptops/desktops

• PDAs/cell phones

• Printers

• CDs/DVDs

• USB thumb driver

Any electronic storage device can be interrogated for evidence.

Digital Evidence

Three types of digital evidence:

1. Computer-stored records

2. Computer-generated records

3. Computer-stored AND computer-generated records

Elements of forensics:

1. Identify

2. Preserve

3. Analyze

4. Present

Where does the Evidence Hide?

• Deleted files

• E-mails

• Temporary Internet files

• Image files

• Temporary document files

• Formatted or damaged drives

• Print spooler

DELTED FILES

Why delete does not mean delete:

− First character in file name is changed

− Data on drive remains until overwritten

"Deleting" a file only changes the first character in the file name; the data for the file remains on the drive until overwritten.

E-MAIL

What's in a thread?

− Recovery of all iterations of an e-mail can reveal the entire conversation.

CASE STUDY – SEXUAL HARASSMENT

Case example of e-mail evidence :

∗ Female employee leaves company

∗ Hires attorney

∗ threatens a sexual harassment lawsuit against former manager

∗ Provides e-mail evidence

∗ Manager denies allegations

∗ Electronic investigation initiated

∗ Recovered e-mails support manager's claim that the relationship was consensual, and that her e-mail evidence did not tell the whole story.

∗ Lawsuit dropped – no damages paid

TEMPORARY INTERNET FILES

− Images and text appearing at the top of a webpage and viewable without scrolling.

− All images and text on a webpage are cached to the hard drive (and potentially recoverable), even if the user does not scroll all the way down and view it all.

INTERNET SEARCHES

∗ Search terms are recorded in a term+term+term format, making them easy to identify.

IMAGE FILES

PICTURE HIDING

An image file with its extension changed to a text file will not display properly as an image.

Ex: KittyPorn.jpg renamed as system.txt. NOTES

TEMPORARY DOCUMENT FILES, FORMATTED OR

DAMAGED DRIVES AND PRINT SPOOLER

PROACTIVE MEASURES

Create usage policies for:

∗ Internet

∗ E-mail

∗ Digital asset ownership

∗ Privacy concerns

∗ Disk wiping utilities

DIGITAL INSURANCE

Imaging as Standard Employee Exit Policy:

∗ Deterrence effect on employees

∗ Preserves data

∗ Maintains chain of custody

∗ Alternative to “Pull and Store” (frees up hardware)

Case Studies: Data Forensics Driving Legal Decisions in Court

Theft of Intellectual Property Major biochemistry research organization.

• Team of scientists leave the company

• Launch new organization

• Receive lab funding almost immediately

• Announce breakthrough discoveries

-- Did they take valuable research data with them? --

THEORIES

− Proprietary files were copied to removable media.

− Proprietary files were e-mailed as attachments. NOTES

− Scientists were collaborating on new organization while on company time and using company resources.

RESULT OF PRELIMINARY INVESTIGATION

− NO evidence of removable media (file copying).

− NO evidence of files sent outside the perimeter.

− NO incriminating e-mails on company e-mail server.

ANALYSIS OF TEMPORARY INTERNET CACHE

REVEALED THE SMOKING GUN

− Discovery of Internet-based e-mail accounts.

− Multiple communications between involved parties.

− Multiple e-mails with attached documents.

− Clearly defined plan to leave company, take research documents, and start competing organization.

RESULT OF INVESTIGATION

Analysis of the temporary Internet files revealed

Web-based e-mail accounts through which communications and file attachments were sent outside the company.

Embezzlement

Major Telecommunications Company.

• CSO receives anonymous e-mail from individual claiming of knowledge of $20M theft of calling card PIN codes.

• Informant seeks reward.

PATH OF THE INVESTIGATION – STAGE ONE

TCP/IP tracing

− Identified initial e-mail TCP/IP address. NOTES

− Traced IP address to Internet service provider.

− Subpoenaed ISP for name of individual.

− Determined identity of suspect.

RESULT

Identified suspect as current employee.

PATH OF INVESTIGATION – STAGE TWO

Analysis of suspect office PC

− E-mail analysis

− Internet activity

RESULT

∗ Discovered four additional suspects.

∗ Discovered PIN codes sold via EBay.

PATH OF INVESTIGATION – STAGE THREE

Analysis of network logs.

− Identified narrow window of opportunity for access codes.

− Identified remote log-in times of suspect.

RESULT

∗ Determined how theft occurred

∗ Documented all activities

∗ Law enforcement notified

∗ Suspect arrested

Result of investigation: Criminal conviction.

Corporate Fraud

Enron/Merrill Lynch "Nigerian Barge Deal."

GOVERNMENT ALLEGATIONS

− Enron and Merrill Lynch executives made a deal for a loan, but booked it as a sale to boost profits.

− Defrauded stockholders.

− Received unearned bonuses.

− Artificially boosted stock prices.

− Government evidence against defendants included a document describing the deal in terms contrary to defendants' statements.

PATH OF THE INVESTIGATION – STAGE ONE

Digital investigation

− Defendants' user directories from network server backup tapes were acquired.

− User directories were searched for keywords taken from paper document in evidence:

∗ Damning document (filename unknown)

∗ Keyword search

∗ Found electronic version – determined filename and expanded search

∗ Metadata analysis

∗ Determined: original author, last 10 saves, last 10 "authors," last print time, and totaledit time

PATH OF THE INVESTIGATION – STAGE TWO

− Expanded search using data recovered from electronic version

− E-mail search

− Recovered e-mail with document attached

− Extracted document and compared

∗ Established document history

∗ Identified modifications, when they were made, and by which user

RESULT OF INVESTIGATION

Recovery and analysis of document in its electronic form revealed relevant information that could never have been determined from the paper document alone.

Incidence Response

If an investigation is anticipated – PRESERVATION IS

CRITICAL

 Overwrites can happen with any activity.

 Quarantine the computer if possible.

 Tape a “DO NOT TOUCH” note on the PC.

 DO NOT turn the PC ON or OFF.

 DO NOT start the investigation.

 DO NOT allow access to the PC before it is imaged.

 Treat the device as a crime scene, because it just maybe!

Question No 42. Discuss the Red Flags Red Flags Associated with Cheque Fraud.

• Frequent deposits and checks:

− In the same amounts

− In round numbers

− With checks written on the same (other) bank

• Frequent ATM account balance inquiries.

• Many large deposits made on Thursday or Friday to take advantage of the weekend.

• Large periodic balances in individual accounts with no apparent business.

• Low average balance compared to high level of deposits.

• Many checks made payable to other banks.

• Bank willingness to pay against uncollected funds.

• Deposits not made daily or intact.

• Entity uses receipts which do not indicate mode of payment.

• One or more personal checks in the cash drawer by the fund custodian.

• Deposit timing lags.

• Irregular check endorsements.

• Amount of deposit does not agree with daily activity report.

• Inappropriate access to signature plate.

• Check numbers, payee name, date, and amount don't agree with entries in the check register.

• Voided checks are not retained.

• Checks are issued to individuals for large, even dollar amounts.

• Supporting documentation for checks is not available or has been prematurely destroyed.

• Cash withdrawal with deposit checks drawn on another bank.

There are several tips for businesses to use when cashing business and payroll checks:

• Examine all checks. Insist that the check by signed in front of the clerk. Compare the signature written on the check with the signature on the driver's license or state identification.

• Be particularly careful with large-dollar checks presented by noncustomers.

• Examine all checks for signs of counterfeiting, such as a glossy, "crayonish" appearance and any lack of detail and sharpness.

• Look for signs of alterations or erasures, especially in the signature or numerical and written amounts.

• Compare the bank identification and routing numbers for a match.

• The texture of the check should appear smooth; a rough document might signal erasures.

• Be cautious of information that is typed or stamped.

• All checks, except government issue, should have at least one perforated edge.

• The magnetic ink used for routing codes should appear nonreflective and dull.

• Look for faded colored paper which can indicate that the check has been chemically bleached.

• A color copy might reflect odd colors at times due to a failure of the toner to mix satisfactorily.

• Black lettering might have a slightly greenish cast when examined under a magnifying glass.

• A light colored or delicate background might fade out when copied.

• Absence of any design in background of check paper.

• Absence of bank logo and the printing of the bank name in regular lettering.

• Absence of the address of the bank on the check.

• Overall appearance of poor quality of printing and paper.

• A payroll check usually will be for an odd amount and will appear neat, clean, and usually unfolded.

• Tellers should telephone the business or account officer for approval on suspicious requests.

Question No 43. Discuss the Common Loan Fraud Schemes.

Ans:

Loans to Nonexistent Borrowers

False applications, perhaps with inaccurate financial statements, are knowingly or unknowingly accepted by loan officers as the basis for loans. These types of loan fraud can be perpetrated by people either external to the lending institution ("external fraud") or by officers, directors, or employees of the victim institution ("internal fraud").

Sham Loans with Kickbacks and Diversion

Loan officers sometimes will make loans to accomplices who then share all or part of the proceeds with the lending officer. In some instances, the loans are charged off as bad debts; in other instances, the bogus loans are paid off with the proceeds of new fraudulent loans.

Double-Pledging Collateral

Borrowers pledge the same collateral with different lenders before liens are recorded and without telling the lenders.

Reciprocal Loan Arrangements

Insiders in different banks cause their banks to lend funds to the others, or sell loans to other banks with agreements to buy their loans—all for the purpose of concealing loans and sales.

Swapping Bad Loans—Daisy Chains

In a daisy chain, a bank buys, sells, and swaps its bad loans for the bad loans of another bank, creating new documentation in the process. Its purpose is to mask or hide bad loans by making them look like they are recent and good.

Linked Financing

Large deposits are offered to a bank (usually brokered deposits) on the condition that loans are made to particular persons affiliated with the deposit broker. High returns are promised, but the

loans are longer term than the deposits (hot money). Sometimes kickbacks are paid to the broker or banker.

False Applications with False Credit Information

Sometimes loan applicants provide false information about their credit situation, and/or overstate their assets.

Single-Family Housing Loan Fraud

In this scheme, unqualified borrowers misrepresent personal creditworthiness, overstate ability to pay, and misrepresent characteristics of the housing unit.

Construction Loans

Construction lending has different vulnerabilities than other permanent or interim lending. More risks are associated with construction projects than with already-built projects. Construction fraud schemes are numerous; the more common are related to estimates of costs to complete, developer overhead, draw requests, and retainage schemes.

Red Flags of Loan Fraud

There are several red flags of loan fraud. Many times the schemes are perpetrated in tandem with other schemes, so what appears to be a red flag for one scheme, might in fact lead the fraud examiner to one or more schemes.

Nonperforming Loans

Although this information might not be available to all, a nonperforming loan is not performing for some reason. One of those reasons might be that a fraud scheme has or is occurring.

Fraud schemes resulting in a nonperforming loan include:

• Fraudulent Appraisals—The cash flow cannot support an inflated loan and, therefore, debt amount.

• False Statements—The loan was made on false or fraudulently presented assumptions.

• Equity Skimming—There was never any intention to make the underlying loan payments.

• Construction Overbudget Items—The overbudget amount might be a concealment method for other schemes such as embezzlement, misappropriation, or false statements.

• Bribery—The loan was made because the lender received a bribe or a kickback from the borrower.

• Land Flips—The purpose of the loan was to finance the seller out of a property which has an artificially inflated value.

• Disguised Transactions—Transactions that are sham transactions, without substance, made to conceal other ills.

High Turnover in Developer's Personnel

One of the first signs to look for, particularly in construction lending, is whether or not the real estate developer is experiencing a higher-than-normal employee turnover. Typically, when a developer experiences a high degree of turnover, something is wrong with the internal operation. This is often a preamble for other problems to come.

High Turnover in Tenant Mix

If the tenant mix in a commercial project (such as a retail center or an office building) is suddenly undergoing a major change, there might be some problem with the management of the project or with the method of allocating the pass-through expenses, such as utilities, maintenance, etc. In addition, a decline in the tenant mix might be an indication that the deferred maintenance for the project is not being properly attended to.

Increased Change Orders

An increase in the number of change orders or amounts on change orders might be an indication that construction changes have taken place that would alter the originally planned project to such an extent as to render the underwriting inappropriate. Change orders can have the same impact on a project as altering the original documents. As with anything that is contracted for on a bid basis, change orders also could be an indication of collusive bidding. Change orders might be an

indication that the original project was not feasible and short cuts are shoring up other problem areas. Change orders should be approved by the architect and engineer on the project in addition to the lender's inspector.

Missing Documentation

Missing or altered documentation is a red flag for any type of fraud scheme. Because concealment is a key fraud element, missing documents are a definite giveaway. Missing documents are of particular concern in construction lending. Experience has shown that seldom is a complete draw request submitted without some missing document.

LOAN FILE

Missing documents in the loan file are another indication that things might be amiss. It is important to determine if missing documents have been misplaced or were never received. A waiver of certain documents is one common way for lenders to conceal fraud schemes. Documentation for real estate loans is fairly standard. Listed below are some of the more important documents which should be present in the loan files.

• Appraisal

• Architect and engineers' report

• Assignment of leases and rents

• Assignment of limited partnership notes

• Assignment of take-out Commitment

• Attorney opinion Letter

• Availability of utilities (water, sewer, gas, and electric)

• Budget

• Completion schedule

• Copies of leases (existing or if project is preleased, commitment letters)

• Disburser's notice, if required

• Easements

• Environmental impact study

• Ingress and egress

• Inspection report (lender's inspector)

• Insurance binder (lender should be loss payee)

• Letters of credit, if applicable

• List of general and subcontractors

• Loan agreement

• Plans and specifications

• Promissory notes from limited partners to partnership, if applicable

• Road dedications

• Soils report

• Subscription agreements, similar to limited partnership notes, if applicable

• Survey

• Take-out commitment, if applicable

• Title policy, including instruction letter from closing

• Zoning

DISBURSEMENT FILE

• Copies of all checks issued at closing

• Lien releases issued at closing (architect, engineers, etc.)

• Loan closing statement

DRAW REQUESTS

• Draw request form (AIA Form or its equivalent)

• Bank reconciliation (general contractor disbursement account)

• Canceled checks (if general contractor pays subcontractors, copies of the canceled checks should be included in the following draw)

• Inspection report (lender's inspector)

• Lien releases for each subcontractor for the previous draw

• Loan balancing form (the lender should prepare some form of reconciliation to ensure that with each draw the loan remains in balance. Items of particular concern are interest, tenant finish, and retainage.)

• Receipts (for all items submitted on the draw request form)

• Title updates from the title company

• Wire transfer instructions (from the lender to the general contractor's disbursement account

In addition to the normal loan files, the lender should require a continuing report from the borrower. For example, the borrower could be required to report annual financial condition coupled with a tax return. Missing documents in these follow-up files might indicate that the project or the borrower is having difficulty that might be the result of a fraud scheme.

Loan Increases or Extensions, Replacement Loans

A loan being continually extended and loan increases being made simultaneously might indicate that the real estate project cannot support the debt service. Typically, the loan increases are to pay for the interest and extension fee. This red flag also might indicate that the loan was made to a related-party or made as a loan to hasten a sale or other transaction. In other words, the loan was not properly underwritten.

If the loan is increased and extended several times, it might indicate that higher appraisals are being obtained on a "made-as-instructed" basis. Loan increases and extensions might be the method used by the lender to conceal a nonperforming loan.

However, according to William T. Thornhill, CFE, a consultant in the field of financial institution fraud, fraud perpetrators tend to write a new loan or credit facility to replace an existing or old loan because they are aware of the fact that a rewrite may attract loan review, loan administration, or internal audit attention. Accordingly, replacement loans are now increasingly used rather than a simple rewrite of a loan.

Cash Flow Deficiencies

The actual cash flow of a commercial project is a very telling red flag. If the project is experiencing an unexplained cash flow deficiency, then an internal fraud scheme might be the cause. The project cash flow might reflect any of the above schemes.

Change in Ownership Makeup

A change in the ownership makeup, commonly referred to as business divorce, might indicate fraudulent activity. It is not uncommon to have a working partner and an equity (money) partner. When the two partners become disenchanted with their relationship and seek a "separation," it might suggest things have gone sour.

Disguised Transactions

Transactions disguised to conceal their true nature often involve the lender and either an existing customer or new customer. Banking personnel sometimes will engage in fraudulent schemes to

forego the requirement to record additional loan loss reserves. One method employed is to "sell" OREO (Other Real Estate Owned) property to an existing customer or a new customer in exchange for making a new loan on an other unrelated project. In other words, the bank is tying one transaction to another, quid pro quo.

Another method of concealing the true nature of a transaction is to conduct the transaction through nominees. For example, the bank might be required to recognize an additional loan loss reserve due to the lack of performance on a particular loan. The borrower might or might not be a good customer of the bank. Regardless of the status of the customer, the bank might request that the project (underlying collateral) be sold to another party, the financing to be arranged by the bank. The borrower can form a new entity (nominee or shell company) to purchase the property; a new (generally higher) appraisal is obtained and the property is sold. In this illustration, the avoidance of loss required the participation of the bank personnel, the borrower, and the appraiser.

Question No 44. What is meant of Embezzlement and explain the Embezzlement Schemes.

Ans:

Embezzlement is defined as the wrongful taking or conversion of the property of another for the wrongdoer's benefit. Misapplication often accompanies embezzlement, but is a separate and distinct offense. Misapplication is the wrongful taking or conversion of another's property for the benefit of someone else.

Types of Embezzlement Schemes

There are various embezzlement schemes which have been utilized over time. The following examples are not an exhaustive list, but are rather a summary of the more commonly employed schemes.

False Accounting Entries

Employees debit the general ledger to credit their own accounts or cover up customer account thefts.

Unauthorized Withdrawals

Employees make unauthorized withdrawals from customer accounts.

Unauthorized Disbursement of Funds to Outsiders

Employees cash stolen/counterfeit items for outside accomplices.

Paying Personal Expenses from Bank Funds

An officer or employee causes bank to pay personal bills, then causes amounts to be charged to bank expense accounts.

Theft of Physical Property

Employees or contractors remove office equipment, building materials, and furnishings from bank premises.

Moving Money from Customers' Dormant or Inactive Accounts

Persons with apparent authority create journal entries or transfer orders not initiated by customers to move money among accounts. Dormant accounts are defined by the Encyclopedia of Banking and Finance as "bank or brokerage accounts showing little or no activity, presumably with small and without increasing balances." Contact with the account holder by confirmation, letter, or telephone contact is not possible. Such accounts are to be transferred to dual control and recorded in an inactive accounts ledger. State statutes usually provide for escheat or forfeiture to the state after a period of years.

An inactive account is defined as "an account with a bank which shows a stationary or declining balance and against which both deposits and withdrawals are infrequent; or an account with a broker which shows few transactions, either purchases or sales." If the bank cannot establish contact with the account holder, then the account would qualify as a dormant account as defined above. However, if there is a risk of misuse of the account, such as an account holder who is quite elderly or incapacitated, then the account should be classified as an inactive account.

Unauthorized, Unrecorded Cash Payments

A director, officer, or employee causes cash to be disbursed directly to self or accomplices and does not record the disbursements.

Theft and Other Unauthorized Use of Collateral

Custodians steal, sell, or use collateral or repossessed property for themselves or accomplices.

Detection Methods There are several methods by which embezzlement can be detected. Generally, if the dollar amount of the embezzlement scheme is small enough such that the financial statements will not be materially affected, embezzlement fraud can be most effectively detected through the review of source documents. If the scheme is so large that the financial statements of the institution are affected, then a review of the source documents will serve to confirm or refute an allegation that an embezzlement scheme has occurred, or is occurring.

Generally, for large embezzlements, the most efficient method of detection is an analysis of the financial statements (which is also a review of documents).

Question No 45. Discuss the Fraud Prevention and detection for the Credit Card.

Ans:

The essential part of any detection program is the education of the tellers and merchants who are responsible for handling the transactions. In a study by Money Magazine, it was found that 95% of store clerks and cashiers did not check credit card signatures.

While any of the following can occur in a perfectly legitimate transaction, these characteristics frequently are present during fraudulent transactions. Tellers and merchants should be advised to be alert for the customer who:

• Takes a card from a pocket instead of a wallet or purse.

• Purchases an unusual number of expensive items.

• Makes random purchases, selecting items with little regard to size, quality, or value.

• Makes several small purchases to stay under the floor limit, or asks what the floor limit is.

• Does not ask questions on major purchases.

• Signs the sales draft slowly or awkwardly.

• Charges expensive items on a newly valid credit card.

• Cannot provide photo identification when asked.

• Rushes the merchant or teller.

• Purchases a large item, such as a television console, and insists on taking it at the time, even when delivery is included in the price.

• Makes purchases and leaves the store but then returns to make more purchases.

• Becomes argumentative with the teller or merchant while waiting for the transaction to be completed.

• Makes large purchases just after the store's opening or as the store is closing.

Merchants should also be aware of potential signs of fraud in card-not-present transactions:

• Larger than normal orders.

• Orders that include several of the same item.

• Orders made up of "big-ticket" items.

• "Rush" or "overnight" shipping.

• Shipping to an international address.

• Transactions with similar account numbers.

• Shipping to a single address, but transactions placed on multiple cards.

• Multiple transactions on one card over a very short period of time.

• Multiple transactions on one card or a similar card with a single billing.

• In on-line transactions, multiple cards used from a single IP (Internet protocol) address.

• Orders from Internet addresses that make use of a free e-mail service.

Tellers and merchants should be aware of the common signs of forged credit cards:

• Holograms crudely stamped or badly faked with tiny bits of aluminum foil.

• Misspelled words on the card.

• Altered signature panel.

• Discolored.

• Glued.

• Painted.

• Covered with white tape.

• Cards which appear to have been flattened and restamped.

At the consumer level, the credit card user should remember the following:

• Know where your card is at all times.

• Never leave your card unattended at work—There are more credit card thefts in the workplace than in any other single situation.

• Don't leave the store or ATM without all of the copies and carbons.

• Don't leave your card in plain sight where others can get the number.

• Don't leave receipts in a public trash can, hotel, or shopping bag.

• Review monthly statements for accuracy and any items that you might not have charged.

• Review your statements via electronic means rather than waiting for paper statements. If possible, cancel paper statements altogether since most fraudsters still practice "dumpster diving" and will riffle through your trash for old receipts and credit card statements.

• Sign the back of a new card as soon as you get it and destroy old cards that are outdated or no longer used.

• Make a list of all of your cards and their numbers. This key information is helpful when reporting lost or stolen cards. Store this list in a highly secured area.

• Be wary of offers that come through the mail.

• Never reveal your number over the phone to anyone who has offered you a prize

• Report missing cards immediately.

• Don't reveal personal information such as your address and telephone number.

• Don’t allow the salesperson to record your credit card number on your check.

• Keep your card out of the view of others in a store or at public telephone so they cannot read the name and account number.

• Use a tiered, see-through container in your wallet for credit cards, so it will be easier to notice missing cards.

• Always check your card when returned to you after a purchase. Make sure it is your card.

The End