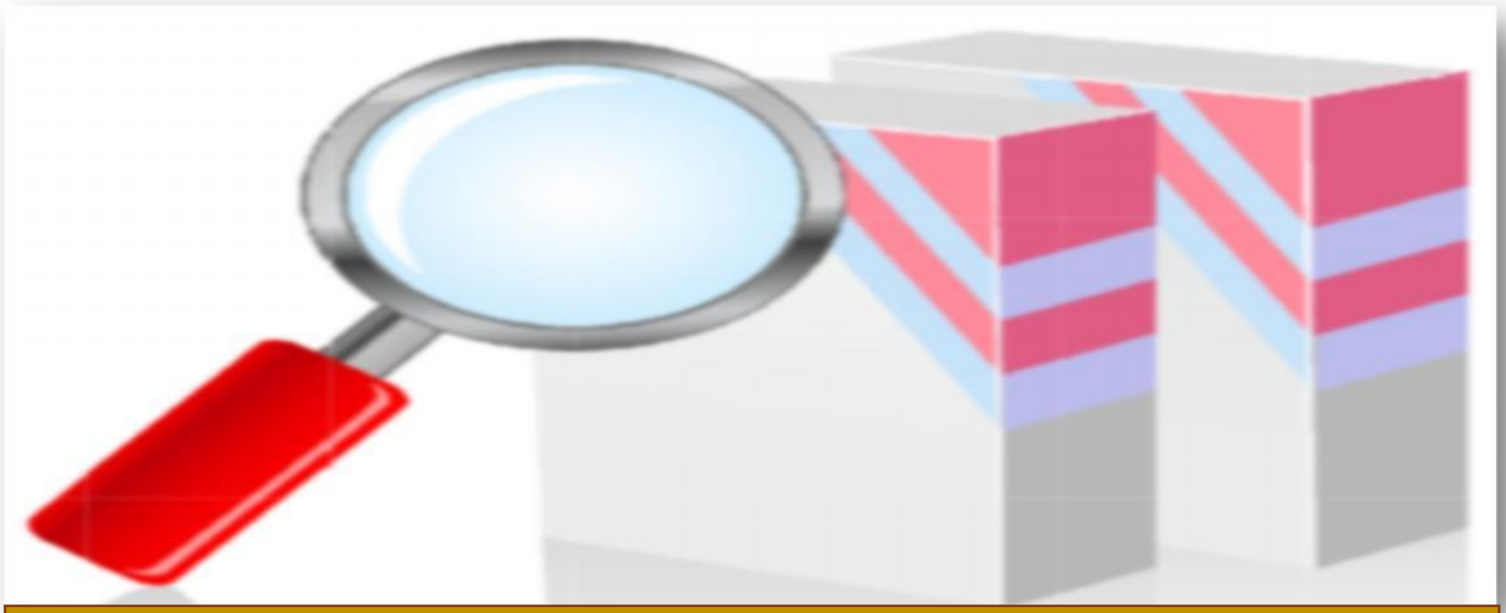


UNIT-9 Fraud Prevention

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Examine the Enforcement of Ethics and Fraud prevention Strategies
- ✓ Explain the importance of having Fraud Policy for a business

Unit 9

Fraud Prevention

It is difficult to determine what to protect and how to protect it while developing a fraud control system. Forensic accountants need to perform a risk assessment first in order to identify risks other than the fraud that has already occurred. This risk assessment would include high-risk assets, fraud schemes that are most likely to occur, fraud indicators, and residual risk after assessing the controls that are in place to check fraudulent activities. Fraud prevention and risk assessment are two different topics of discussion, and each deserves a thorough understanding.

An anti-fraud program is intended not only to detect fraud but also to prevent it. Detection and prevention are linked to each other and constitute an important part of the anti-fraud system. This unit discusses the components of a successful and efficient anti-fraud control system.

Prevention Environment

Analyzing the entity's culture and changing it (if necessary) is important if fraud prevention is to be successful. There are certain activities and attitudes that can help in achieving this goal. Discussed below are some important prevention elements that are generally applied to the entity and are not targeted at a specific fraud.

Corporate Governance Structure

According to research, weak corporate governance has played a role in all major financial frauds. In 1998, the COSO Landmark Study examined 200 out of 300 fraud cases handled by the Securities and Exchange Commission (SEC) between 1987 and 1997. This study revealed that all entities that were investigated had weak boards. In 72% of cases, the Chief Executive Officer (CEO) was identified as being involved in the fraud. In 43% of cases, the Chief Financial Officer (CFO) was similarly identified. Moreover, according to Wheel, Deal and Steal, former or current CEOs head the majority of boards.

The report identified the following weaknesses:

- Dependent board members
- Insiders dominating the Board
- Significant equity holdings by board members
- Inexperienced board members
- No communication or meetings between board members and audit committees
- Inexperienced and untrained audit committee members
- No audit committee
- No meetings held by the audit committee

- Top executives involved in the frauds

The basic elements of governance are clear from the weaknesses listed above. For example, it is clear that audit committees are responsible for setting up and implementing complaint and whistle-blower systems that also act upon anonymous tips. Therefore, it can be concluded that good corporate governance requires active, qualified and independent members of the board and of the audit committee.

Tone at the Top

Management is responsible for setting the tone in the organization's environment. The tone at the top is a key factor in fraud prevention, regardless of the organizational structure. In almost every fraud case in recent years, an executive was involved in the fraud. The executive involved in the fraud distrusted people and kept important financial information from the auditors. Therefore, in organizations such as Enron, WorldCom, Tyco and others there was a lack of an anti-fraud tone at the top management level. An anti-fraud culture is established in organizations where top managers and the board of directors consistently talk about fraud, communicate fraud policies to employees, and encourage everyone to actively participate in fraud detection and prevention. It is impossible to develop an anti-fraud culture without constant effort and emphasis by key management.

Realistic Financial Goals

The setting of over-optimistic and unrealistic performance goals was another element in major frauds. Every organizational objective revolved around achieving abnormally high profits in entities that encountered financial fraud. The company's board of directors should avoid setting unrealistically high financial targets in order that the managers and other executives do not have to resort to fraud and deception to achieve those targets. Reaching a balance between financial objectives and their negative impact is an important and delicate task. Pressure and unrealistic targets constitute one leg of the fraud triangle while opportunity is the second. Management always has the opportunity to collude with those committing the fraud and override internal controls. Rationalization is the third and final leg, which involves the executives' ethics and has the ability to prevent a person from committing fraud even if the first and second legs exist.

Policies and Procedures

The objectives and principles of an entity are its policies, while the organization's actions taken to ensure that objectives are achieved are called procedures. Policies and procedures document all unethical actions and transactions and determine how violations should be treated. A sound fraud policy and procedures based on that policy contribute substantially to laying a firm foundation for an anti-fraud environment. All publically traded companies are required to have an ethics policy as per SOX, while

companies without an ethics policy are required to state the reasons for its absence. Policies define entity objectives and principles, while procedures define actions taken by the entity to ensure that objectives are achieved. Policies and procedures document the actions and transactions determined to be unethical, as well as stating how violations will be treated. The company's fraud policy is a source indicating the company's fraud prevention measures, actions that have been taken to detect and respond to fraud, and the efficacy of the anti-fraud environment.

The company's policy and procedures should have the following characteristics in order to develop an effective anti-fraud culture:

- Define frauds
- Publication and communication of policy
- Describe how anti-fraud controls would be implemented
- Describe training
- Describe proactive audit measures to detect and prevent fraud
- Describe how anti-fraud controls are tested
- Define investigation policies and procedures
- Describe actions taken in fraud audit
- Describe how evidence is analyzed
- Describe ways to resolve fraud
- Describe procedures used for incident reporting

For an effective anti-fraud system, a written fraud and ethics policy alone is insufficient. It is necessary to communicate this policy to all related parties and implement it. This can be done by including ethics and fraud in employee orientation programs. An active monitoring and compliance system is vital for the success of a fraud policy. Research conducted on fraud statistics revealed that a combination of all three factors — policy, communication, and compliance — led to significantly lower instances of fraud.

However, only one tenth of the companies with a written fraud policy also have an active compliance mechanism. An ethics policy does not necessarily have to involve a long list of policies and procedures; rather, it may be simply based on values and principles that are symbolic for the entity. These values must be firmly incorporated into employee behaviours and organizational culture, and these must be reinforced by actions. It is important for an organization to take the human element into consideration when developing a culture. While there are numerous factors that influence organizational culture, some are clearly more important than others. Human resource is a significant component in determining organizational culture. Therefore an anti-fraud culture that caters for the people, the business operations, and the organization as a whole may ensure that fraud risk is minimized.

Perception of Detection

Perception of detection is one of the leading elements in fraud prevention. According to crime experts with years of experience in law enforcement and criminal justice, the perception of detection is the biggest deterrent to any kind of crime, including fraud.

The fear of punishment, imprisonment, humiliation, and the loss of personal relationships are enough to make a potential fraudster think several times before committing fraud and evaluate whether it is worth all the risk or not. This technique for deterring fraud is more effective in financial fraud cases than in street crime because most white-collar criminals follow their own personal ethical codes. Therefore, increasing the perception of detection is the best, most cost-efficient way of minimizing the risk of fraud. Tactics for increasing the perception of detection include:

- Surveillance
- Anonymous tips
- Surprise audits
- Prosecution
- Enforcement of ethics and fraud policies
- Catch me if you can!

Fig. 9.1

Surveillance

Surveillance cameras might be installed in places such as mailrooms, where mail containing cheques or cash is opened, and where assets are subject to high risk, in order to increase the perception of detection. In addition to installing surveillance, it is important to announce that such measures have been taken, thereby rendering it effective in preventing fraud. For surveillance to be a success, it is important that people believe that someone is actually watching and monitoring their activities. Unethical employees and potential fraudsters will first test the efficacy of such monitoring and determine whether suspicious activities are followed up or not. The use of fake cameras can be effective but only in conjunction with live cameras and speedy follow-ups.

Anonymous Tips

Following up on anonymous tips is one of the best methods of fraud detection, as well as prevention. If employees and potential fraudsters are aware that anyone may turn them in and that they are constantly being watched, this fosters a very strong perception of detection. Appropriate involvement of management, involving a third party to independently handle complaints, and employing multiple communication methods such as telephones, letters, and e-mails are among the effective practices that might be incorporated in anonymous tip programs. Employees should be provided with an easy, convenient and safe path to offer tips.

Surprise Audits

According to the Association of Certified Fraud Examiners' [ACFE] Report to the Nation [RTTN] statistics, the internal audit is the highest ranked, proactive method of detection. However, surprise audits conducted by internal or hired auditors is an even more effective method. These methods are effective for more than just fraud detection; the mere announcement that an audit might take place at any time creates a perception of detection.

Fraudsters do not have the time to prepare deceptive answers for the auditors, as they do not know when the audit will occur. In one instance, for example, the internal auditor played a joke and announced a surprise audit, which led to the manager confessing to a fraud.

Prosecution

Prosecuting fraudsters to the maximum extent of the law sends a strong signal that no one can get away with financial crimes. However, there is risk associated with public trials and the possibility of the prosecuting agency failing to do its job. According to most experts, prosecuting fraudsters is the key to maintaining a perception of detection. One the one hand, it ensures justice for the entity and the fraudster, and on the other it warns potential fraudsters against committing fraud.

Enforcement of Ethics and Fraud Policies

An entity should have a clear plan of action in case a fraud occurs, including determining the penalties for different kinds and levels of fraud. Ensuring compliance with the entity's fraud and ethics policy has the same effect on the perception of detection as that of prosecution and surprise audits. The entity must ensure that it imposes the punishment laid down in its policy. Inability to conform to its own policy would be worse than the organization having no policy at all. Moreover, it is best to establish such policies and penalties beforehand, as making such decisions after the fraud has occurred can be difficult and may not result in the best possible decision.

Catch Me If You Can!

The greatest perception of detection is to catch the fraudster, prosecute him/her according to the law and organizational policy, and publicize the treatment of the fraudster. Recent examples of successful fraud detection serve as a message that the entity is not only capable of detecting fraud but is also willing to prosecute those who commit it, in addition to rewarding those who helped detect fraud and contributed positively to the anti-fraud culture.

Classic Approaches

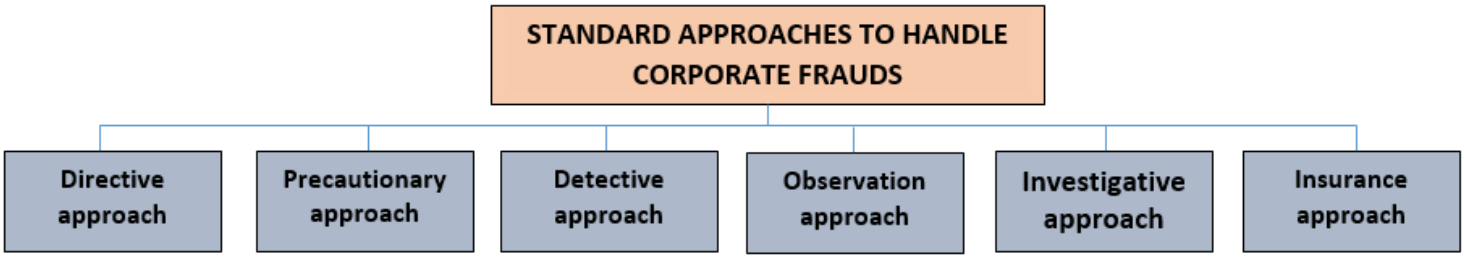


Fig. 9.2

Reviewing the classic approaches adopted to reduce employee theft, fraud and embezzlement will help to develop an efficient fraud prevention program. The following are some of the classic tactics:

- **Directive approach.** This is a confrontational and authoritative approach, clearly stating that if someone steals, they will be caught and fired from their job. In taking this approach, the entity does not take measures to prevent fraud. If a fraud occurs and is detected, the accused is simply fired without a prosecution. In such a case, the management itself would be shocked to learn that someone had committed a fraud.

- **Preventive approach**. According to this approach, preventive measures are taken to screen out potential fraudsters; these measures include background checks for previous criminal records and credit reports. Active and efficient internal controls also contribute to fraud prevention. Segregation of duties to the extent that the management must override controls or people must collude in order to commit fraud is also a tactic used in the preventive approach.
- **Detective approach.** This entails setting up strong accounting controls and an internal audit function to monitor transactions against potential frauds. The internal audit function is responsible for periodically verifying the legitimacy of transactions and confirming that the entity's assets exist. Accounting controls are established to detect any fraud that may occur in between periodic audits.
- **Observation approach.** This approach is dependent on the physical observation of assets and employees. Management is responsible for monitoring employee conduct and looking out for suspicious behaviour and activities. Cameras and other kinds of in-person surveillance are used to monitor the level of stock and quantity of valuable portable goods, such as cash and valuable inventory.
- **Investigative approach.** This approach follows up on the discrepancies revealed after investigation. It includes following up on allegations of theft, and unfavourable or favourable variances in inventory, goods, materials, supplies, and costs. The entity will investigate and determine the nature and extent of the loss and the people who are suspected of committing the crime.
- **Insurance approach.** This is dependent on adequate insurance coverage to make up for the losses that may occur due to fraud. While this approach does nothing to reduce the possibility of employee fraud, it certainly softens the financial repercussions of a financial crime.

Other Prevention Measures

There are other measures, apart from the general environmental, cultural and corporate measures, that might minimize fraud. Preventive measures and fraud countermeasures should be focused on people who have access to or control over sensitive assets such as cash and cheques. Appropriate countermeasures must ensure that these employees will be held accountable for handling valuable assets.

Background Checks

Making background checks on key employees is another preventive measure. Although it is not a 100% effective method and may even be costly, it can still reveal important background information about employees. It can reveal a past criminal record, high debt, etc. Either of these facts may dissuade the management from hiring the employee. High debt means that economic and financial pressure is present, fulfilling one of the legs of the fraud triangle. A criminal record is an indication that the

employee has a history and willingness to commit fraud and the ability to rationalize his/her actions. This fulfils the rationalization leg of the fraud triangle.

As per ACFE 2008 RTTN, a mere 7% of fraudsters had prior convictions, while 12% had a prior history of being dismissed by their employers for being involved in fraud. Calling up a potential employee's references is also an effective measure that is often overlooked. There have been instances of fraudsters making mistakes when providing references or being over-confident that the referees would not be contacted. In these cases, a simple phone call had greatly influenced the hiring decisions.

Regular Audits

Regular visits by auditors are an effective prevention measure. While the main aim of the audit is detective by nature, it still creates a strong perception of detection and can therefore serve as a prevention measure. Identifying, reviewing and analyzing anomalies are important if regular audits are to be effective, and if the auditors use their tools to pursue fraud aggressively, regular audits become more effective as a prevention measure.

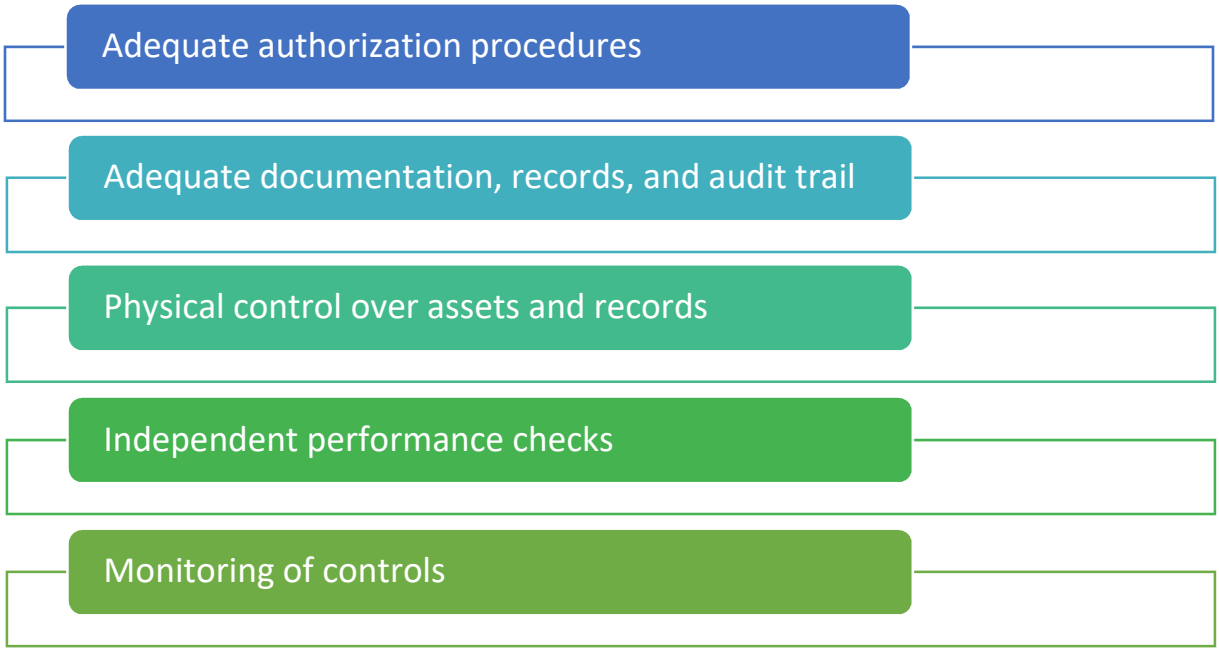
In major financial frauds of recent years, the internal audit function was not allowed to function to its full potential, as financial information was not analyzed and other kinds of frauds were investigated. The CEOs of those companies did all they could to prevent diligent auditors from investigating their scams.
Only when an auditor came in late at night to examine financial records that the executives were not willing to provide were the fraud and the CEO involved in it exposed.

In another instance, a small university newspaper office in the USA employed one accountant to perform all accounting functions while a retired accounting professor was responsible for performing regular audits of the office. One year, in April, the professor notified the university that he would be performing his final audit and that they should arrange for a new auditor or put their internal audit function into effect. The university did not have an internal audit function. The university VP received a call from the newspaper-printing vendor in mid-October. The university was informed that the company would not be printing the next issue of the newspaper, as they had not been paid in some time. Upon checking the accounting records, it was revealed that the accounting clerk had been stealing thousands of dollars. The theft had begun in May of that year, after the auditor had left. It was clear that the regular audits of the newspaper office served as a perception of detection and prevented the clerk from stealing. Once the threat of audit was removed, the clerk was able to rationalize the fraud.

Internal Controls

Opportunity is one of the elements of the fraud triangle, referring essentially to internal controls. Fraud auditors have little impact on the other two legs of the fraud triangle, i.e. pressure and rationalization, although management can create an enabling environment for these elements. Pressure and rationalization are psychological and are therefore difficult to observe. Internal controls, on the other

hand, are more easily observed and may influence the opportunity to commit fraud. One of the most common internal control lapses is the lack of segregation of duties. The following are some internal control activities that might serve as preventive measures:



Invigilation

Invigilation is a variation of surveillance. During invigilation, the fraud auditor is responsible for creating a fraud-free environment through a high-profile, well-staffed fraud audit. The employees will be very careful and ensure that no fraudulent activity takes place during invigilation, and this period provides a benchmark for the amount the company should be earning in revenue. Comparing invigilation period revenues with regular revenues will enable the fraud auditor to determine whether fraud is taking place during regular, non-invigilation periods.

Invigilation is effective where other detective methods fail, for example in cases of off-the-books frauds. Giving management an idea of their likely revenue during the invigilation period enables the detection of skimming and other such fraud schemes that may have gone unnoticed.

Accounting Cycles

Examining business processes and accounting cycles in their natural setting is one way of addressing prevention measures. Analyzing common fraud characteristics during these cycles helps develop effective countermeasures. The following examples show how preventive measures can be affected.

Generalizations

All accounting transactions and accounting cycles are specific to different organizations. The uniqueness of accounting cycles is dependent on the industry, size, organizational culture, structure, capital structure, strategy, etc. In order to detect or prevent fraud, it is important to understand the environment and the situational factors in which the organization is functioning, as no fraud occurs in a vacuum.

The size of the organization is one of the most important factors affecting fraud control. Size has an influence on the segregation of duties, which is a key factor in fraud control. The type and amount of fraud are also affected by size. When determining control methods, size is always a consideration, as large organizations tend to be more complex and are difficult to control. However, larger organizations have more resources to spend on fraud control. Smaller organizations have the opposite characteristics. This generalization does not always hold true. Although segregation of duties is more easily observable in small, tightly connected organizations, it is much more difficult to implement as a preventive measure. The importance of understanding the context and fraud environment cannot be overstated.

Despite differences in accounting cycles from one organization to another, similarities do exist. There are only a handful of basic accounting cycles, and although fraudulent transactions may have numerous forms, they are largely the same in substance.

Sales Cycle

Lapping is one of the common fraud schemes related to the sales cycle. For this scheme to be successful, the fraudster cannot take more than one day off work at a time. Forced rotation of duties and forced vacation time are two preventive measures against lapping. Larceny and write-off schemes can be prevented through segregation of duties or by adding an independent authorization step to the business process.

Purchases Cycle

The highest percentage of fraud occurs through fraudulent disbursement in the purchase cycle. The use of shell companies is a common fraud phenomenon. Fraudsters need to add vendor companies to the authorized list for this fraud to be successful. Again, segregation of duties or adding an authorization step can prevent such fraud. These measures are also effective against cheque-tampering, false voids, false refunds, etc. Prevention and detection controls must ensure that transactions with related parties are carefully monitored, as this area is vulnerable to fraudulent disbursements as well.

Payroll Cycle

Setting up ghost employees is a common fraud scheme in the payroll cycle. Employees can be added to the authorized payroll file through an independent party. Regular cross-checking of payroll against HR records is an effective prevention method, as a ghost employee present on the payroll will be missing

from the HR records. Forced rotation of duties and mandatory vacation time for the payroll manager are also important measures. A thorough hiring process that pays close attention to the kind of people associated with the organization is an effective technique for preventing fraud since fraud is committed by people, after all.

Fraud Response

An anti-fraud program consists of three basic phases: prevention, detection and response. Response is necessary after a fraud has been detected. The management should have a pre-planned response in case a fraud occurs and is detected. The response phase is usually the first or second phase (fraud risk assessment comes first) in planning and developing policies and anti-fraud procedures.

Fraud Policy

An appropriate fraud policy is the best starting point for developing an efficient fraud response. This step must be undertaken before a fraud actually occurs or before the specifics of an anti-fraud program are determined. While developing a fraud policy, there are several issues that need to be considered. The first is the definition of fraud.

Let us suppose that an employee "borrows" the employer's camera. This employee uses the camera to take pictures of his/her personal property or personal belongings and then uses the company's computer to set up an eBay account and sell his/her belongings all during work hours. Might this be categorized as a fraud? Without a proper definition of fraud, a judge or jury would struggle to call it a fraud. However, if the entity had used the ACFE's definition of fraud in its fraud policy and made all employees sign it to secure their agreement, there would be much less doubt regarding the term "fraud" in the courtroom.
The same policy could be applied to employees who "borrow" heavy equipment for their personal use over the weekend, as it is not required until Monday. Therefore, it is important that the company craft a definition of fraud and make it a part of their fraud policy. The following should be considered when defining fraud:

- Any dishonest or fraudulent act
- Violation of fiduciary responsibilities
- Misappropriation of funds, securities, supplies, or other entity assets
- Unauthorized use of the entity's assets, such as equipment and computers for personal use
- Improper handling or reporting of money or financial transactions
- Earning profits from insider knowledge of entity activities
- Disclosing confidential and proprietary information to outside parties
- Disclosing securities-related activities of the entity to outsiders
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services or materials to the entity. Gifts worth less than $50 are an exception
  Destruction, removal, or inappropriate use of records (paper or digital), furniture, fixtures, or

equipment

- Malicious activities involving the entity's computers, systems, or technologies
- Any violation of a relevant legal act
- Any similar or related irregularity

The entity's fraud policy should also include the methods management will adopt when irregularities are detected or suspected. It should include questions such as who, what, where, and when in connection with any tips or complaints that are received and to whom such tips should be reported. The policy should ensure that the anonymity of the person providing the tip is maintained. The policy should clearly specify how such reports should be investigated, in addition to avoiding the occurrence of false or mistaken accusations, thereby alerting the suspect that an investigation is underway. Special care should be taken not to disclose any information on the investigation or the status of the investigation unless it is authorized by the management or required for legal reasons.

The policy should be particular about maintaining confidentiality for the sake of innocent employees who may have been swept up into the investigation and for the whistle-blowers.

Fraud Response Team

Once the fraud policy has been laid down on paper, the management should identify the people and positions that are responsible for implementing the various procedures included in the policy. "Fraud Policy Decision" is a tool provided by ACFE to assist management with their fraud response efforts.

Fraud Response Team and SMEs

Legal/Litigation: prosecution, knowledge of potential effectual prosecutors, civil litigation
Legal/HR: legal termination of fraudster, legal issues in investigating an employee
Forensic accounting/CFE: fraud investigation, fraud/legal evidence, proper interviews
Digital forensics: data mining for evidence
Cyber forensics: evidence embedded in IT, hidden in IT, potential cyber sources of evidence
Internal audit: support the investigation, evidence gathering, controls remediation
Public relations: avoid publicity, manage publicity, craft public responses to fraud
Executive management: manage all key decisions of the process and follow up

A Subject Matter Expert (SME) is a requirement in any forensic accounting-related activity or fraud investigation. Some people tend to confuse a fraud audit with a financial audit and think that an internal auditor or a financial audit expert will be able to carry out a fraud investigation or audit for evidence. That is a misconception. The approach to a fraud audit is totally different from that to a financial audit, and someone who is not trained or insufficiently experienced to conduct a fraud investigation will not be able to do so successfully. Executive management is a key part of a response team, as senior management should be involved in important decision-making during the investigation and in taking remedial actions in order to prevent fraud in the future. Recovering monetary loss resulting from the fraud and appointing people for that process is an important management decision. When appointing someone to represent the executive management, the fact that the fraud may have been perpetrated by someone from the management should be taken into account.

A person who is able to take on multiple responsibilities might perform some of the team functions; for example, the internal legal counsel might also handle other legal issues related to litigation and HR. The entity can also hire a person who is an SME in cyber forensics and digital forensics. The team might also merge risk management with executive management. While some companies may not possess the units indicated above, they might still benefit from the matrix and gain an idea of the issues that should be reviewed. The matrix also emphasizes the segregation of certain activities if this is feasible.

Recovery

As pointed out earlier, recovering financial losses is an integral part of the response phase. The amount lost due to fraud can be both significant and difficult to recover. Recovery is often difficult as the fraudster has usually spent the money or hidden it.

Business insurance/bonding, restitution agreements, or civil judgements are among the ways of effecting recovery. Restitution agreements and civil judgements are out of the entity's control and may therefore create obstacles to full recovery. Hence, the most effective and reliable approach to achieving full recovery is through insurance or bonding of key employees.

The insurance provider should be chosen carefully to ensure that it fits the management's wishes in terms of the fraud investigation. Some insurance companies require their clients to hand over the investigation to them completely, as the insurance company has its own forensic team. In this case, the entity would lose control over the response phase, which would prevent it from prosecuting or pursuing civil litigation, although it would still be able to take remedial action and dismiss the employee involved. Some insurance companies simply pay off the obligation without pursuing an investigation. The management should choose an insurance provider based on the amount of coverage, the insurance company's terms and conditions, and the management's own preferences regarding fraud response. A good response plan usually involves an adequate insurance plan together with aggressive litigation to obtain full recovery.

Further Reading:

- ✓ ***Prevention and Detection, (2016), By Zabihollah Rezaee, Richard Riley***
- ✓ ***Financial Fraud Prevention and Detection, (2018), By Michael R. Young***
- ✓ ***Fraud Prevention and Detection: Warning Signs and the Red Flag Syst,(2018), By Rodney T. Stamler, Hans J. Marschdorf, Mario Possamai***