# Fraud Prevention

Unit

10

# Unit 10

# 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**

## Introduction

In any organisation, If risk evaluation is not performed when formulating fraud control it becomes very challenging to know what to protect and how to protect it. Because risk evaluation identifies the areas where risks lie within the organisation. Possible risks include: assets at high risk, fraud schemes most likely to occur, related red flags and the residual risk. Both fraud prevention and risk assessment deserve a detailed debate; therefore, they will be discussed separately.

The aim of every antifraud programme is to prevent fraud, not simply to detect it. Detection and prevention are interrelated, and work together to provide the system of antifraud controls. In this unit we will discuss the components that form a successful antifraud control system.

## Prevention Setting

Effective fraud prevention is developed by understanding the entity's culture and changing it if necessary. This goal can be achieved through some approaches and activities. The important prevention elements that are discussed here are not essentially directed toward a particular fraud, but are generally applied to an entity.

### Corporate Governance Structure

Research shows that all leading financial frauds are related to weak corporate governance. An example is the COSO Landmark Study (1998) that studied 200 out of 300 fraud cases investigated by the Securities and Exchange Commission (SEC) from 1987 to 1997. The investigators identified a distinctive pattern whereby all these companies had weak boards. In 72% cases, the chief executive officers (CEO) and in 43% cases the chief financial officers (CFO) were identified to be involved in the fraud. Additionally, according to Wheel, Deal and Steal, most boards were directed by a former or current CEO.

Flaws and weaknesses stated in the report were summarized as follows:

- The board members are not independent.
- The board is controlled by insiders.
- The board members have significant equity ownership.
- The board members have less board experience.
- Audit committee members who knew very little about auditing or finances.
- Boards and audit committees do not meet frequently.
- Top management is involved in frauds.
- Audit committee does not exist.

From the weaknesses and flaws listed here, the elementary components of governance are clear. For example, audit committees are responsible for setting up a system for anonymous complaints and tips, and whistle-blowers. To summarise, good corporate governance contains independent, active and qualified members of the board, particularly the audit committee.

### The Top Management

Irrespective of the corporate governance in the organization, the management's style establishes the character of the organization. Although misused and often ignored, the phrase that 'the tone at the top is key to fraud prevention' is true. If we review the major scandals in recent years, we will discover that an executive was involved in almost every case. That executive usually mistrusted people and tried to conceal the financial affairs from auditors. Thus there was obviously no antifraud system at the top in Enron, Tyco, WorldCom, and others. If key managers and the board of directors continually talk about fraud, inspire everyone to be involved in preventing and detecting fraud, and communicate fraud policies, then the entity will ultimately develop an antifraud system. It is nearly impossible to have such an organizational culture without the support of key management.

### Realistic Financial Goals

A common constituent of major frauds were the overoptimistic objectives set for corporate performance. In most financial frauds of the past, almost every strategy and goal revolved around increasing profits to an abnormal level for that company or industry. If the top management , particularly the board can avoid setting unrealistic financial goals there will be less pressure on executives to reach to those financial goals . One of the elements of the fraud triangle is pressure (motivation), and unrealistic financial goals inevitably create the pressure to commit fraud. Management always dominates controls or plans at some level. Opportunity is the second element of the fraud triangle, which means that if unrealistic performance goals do exist, only the executive's ethics will prevent that executive from committing a financial fraud.

### Procedures and Policies

Procedures define actions while policies define the entity's objectives and principles. The entity takes suitable actions to achieve these objectives. The groundwork for an antifraud

system and environment for any entity is a fraud policy that is carefully constructed. SOX fundamentally requires publicly-traded companies to have a well-defined policy on ethics. Companies without a written ethics policy must explain why they do not have one and state this in their 10-K forms. A fraud policy becomes the source document for developing fraud prevention procedures, actions in response to a fraud, and actions to detect fraud, and thus influence the efficacy of an antifraud climate or culture.

In order to establish an effective antifraud system, an entity must have procedures and policies which:

- Define frauds
- Describe implementation of controls for antifraud
- Describe publication and communication of policy
- Describe training
- Describe event reporting procedures
- Describe testing of antifraud controls
- Describe proactive fraud audit measures
- Define investigation policies and procedures
- Describe the examination of evidence
- Describe actions taken in fraud audit
- Define resolutions to frauds

Creating a written policy for fraud or ethics is not adequate by itself. Effective systems include a means of communicating the policy appropriately to all those involved. An effective strategy would be to include ethics and fraud awareness in employee orientation programmes. A continuous monitoring and compliance system is essential for the success of the policy. It was discovered through research about cooperatives and frauds that when all three elements, namely, policy, compliance and communication were present, fraud cases were statistically considerably less than in any other situation.

Merely about one-tenth of the entities that had an ethics policy had any compliance mechanism in place. Policies about ethics may be based on principles or values. A few values are selected as representative of the entity instead of a detailed list of policies and procedures. With this strategy, employees have to accept the values which must be embedded in the culture and strengthened by action. Essentially, entities must consider the human element of the organization’s system. Although a countless number of factors influence a system, some are more significant than others. The people are a large component of any organizational culture. Building an antifraud system that fits the people and business operations, and the organization as a whole will make certain that fraud is mitigated to the whatever extent possible.

## Perception of Detection

According to antifraud professionals, 'the perception of detection' is the most important element of fraud prevention measures. Crime experts with years of experience in law enforcement and criminal justice say that the best deterrent to crimes, including fraud, is the perception of detection. This technique is more effective in preventing financial fraud than it is for street crimes, because white-collar lawbreakers who commit such fraud tend to have some personal code of ethics. Many potential fraudsters usually stop, think, and decide that the fraud is not worthwhile because of the fear of humiliation, jail, or loss of family ties. The entity can minimize the risk of fraud by increasing the perception of detection in a cost-beneficial way. Some techniques to increase the perception of detection are:


Fig: 10.1

## Surveillance

Surveillance cameras or other surveillance methods can be a good perception of detection method in places where assets are at high risk, such as mailrooms where mail that contains checks and/or cash is opened. If surveillance will be used as a countermeasure against fraud, it is best to announce it to everyone that it is in place. The administration must make sure to monitor surveillance in such a manner that people will believe someone is actually following up on doubtful activities. Unethical staff will test the effectiveness of the surveillance to see if it is really being monitored and used by someone to actually follow up on doubtful activities. It is possible to use dead or fake cameras but only in combination with live cameras with monitoring and efficient follow-up.

### Anonymous Tips

Anonymous tips have been identified as the best method for detecting frauds; however, they are also effective as prevention measures. The reason is simple. If employees know that an anonymous tips system is in place and anyone who sees something suspicious can turn them in, it begins to serve as a perception-of-detection preventive measure. Best practices for anonymous tip programmes include applicable involvement of management, using several communication methods (phone, letter, email, etc.), and independent handling of complaints by a third party. Above all, make it easy, comfortable and useful for employees to provide a tip.

### Surprise Audits

According to the statistics provided by The Association of Certified Fraud Examiners [ACFE] Report to the Nation [RTTN], internal audit has the highest rank in proactive methods of detection. However, surprise audits by either the hired fraud auditors or internal audit functions are even more effective. These audits serve a similar purpose in detecting frauds which can then be considered for further preventive measures. Additionally, the fact that the surprise audit was unexpected can create a perception of detection. Fraudsters do not know when the fraud auditor is going to show up, so they cannot prepare to fool the auditor. In fact, in at least one fraud, a fake declaration of a surprise audit (the internal auditor was attempting to play a joke) caused the manager of the business unit to confess to a fraud.

### Prosecution

Substantial advantage can be gained by prosecuting fraudsters to the maximum extent allowed by law. Although it is true that there is some risk in a public trial, and some risk that the prosecuting agency may fail to do its job successfully, but the benefit is not just obtaining justice for the single event and justice for the fraudster. Instead, prosecuting one individual sends a strong message about perception of detection, communicating the fact that if anyone commits a fraud and gets caught, this entity is going to seek prosecution and perhaps imprisonment. Most experts agree that prosecution is critical for maintaining an effective level of perception of detection.

### Enforcement of Ethics and Fraud Strategies

When handling frauds the same philosophy is applicable for compliance with an ethics policy, a fraud policy, and corporate policy. An organization should have established in advance what it would do if a fraud occurred; what penalties would be enforced for what kinds of frauds and stated levels of fraud. Then the organization should ensure that it monitors and implements these rules.

### Catch Me If You Can!

In fraud detection, the most important measure is to catch a fraudster, put them to trial, and broadcast what has been done. A recently apprehended fraudster can increase the perception of detection and functions as a living example and reminder that this organization is capable of detecting and prosecuting those who commit frauds. Additionally, rewarding an employee who helped in detecting fraud also contributes towards an antifraud system.

## Classic Approaches

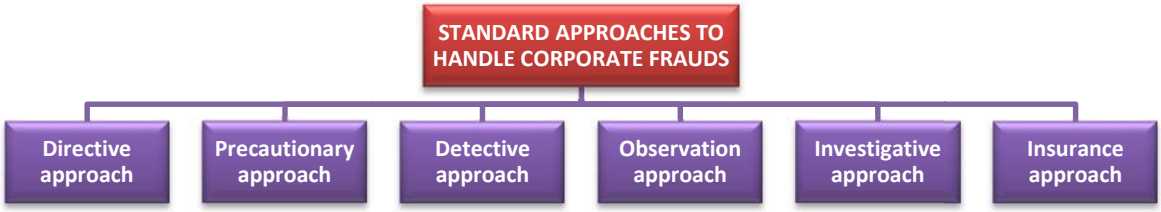


Fig: 10.2

For developing an effective fraud prevention and control programme, a review of the classic approaches towards the reduction of employee theft, fraud, and embezzlement is quite helpful. Here are the examples of standard approaches:

- **Directive approach**: The directive approach is authoritative and confrontational. It sends the message: ‘‘Don’t steal. If you steal, and we capture you, you will be dismissed.’’ An entity that adopts this approach is generally doing little or nothing to prevent fraud. The management would most likely be shocked to know that someone would commit a fraud against the organization. Management would probably fire the employee if a fraud did occur and was detected, and probably would not act further against the fraudster.
- **Precautionary approach:** In this approach, potential fraudsters are identified using various methods, including background checks for credit reports and criminal records. Internal controls can be used in the preventive approach. An example could be segregation of duties which can diminish the risk of fraud at least to the point where persons must conspire to commit fraud or management must override controls, which are always possibilities.
- **Detective approach:** In the detective approach, the management establishes an internal audit function and accounting controls to monitor potential frauds. The legitimacy of transactions is periodically verified by the internal audit function and it also confirms the existence of assets. The management depends on the accounting controls to detect any fraud that might occur between periodic audits.
- **Observation approach:** This approach depends on physical observation of assets and staff members. The management observes employee conduct for suspicious actions or behaviours. Monitoring can be done in person or by other means, such as cameras. The

amount of stocks of valuable and transportable goods, such as valuable and transferable inventory, cash, and other such assets, are also monitored.

- **Investigative approach:** The investigative approaches depend on discrepancies. For example, the organization would follow up on accusations of theft. The entity would follow up to determine the nature and extent of the loss and who the likely criminals might be for certain favourable or unfavourable variations in inventory, goods, materials, purchases, supplies, and product costs.

- **Insurance approach:** The insurance approach is based on insurance coverage that is adequate to cover losses that might occur due to a fraud. This approach moderates the financial shock when fraudulent losses occur but does not reduce employee theft.

### Additional Prevention Measures

In addition to common prevention measures, such as environmental, cultural, and corporate prevention measures, specific prevention measures can be used to reduce the risk of fraud. The important employees are those responsible for prevention measures and fraud countermeasures. These employees also have control or access over valuable and transferable assets, such as cash or checks. An entity should consider suitable prevention measures that would hold these employees accountable for handling valued assets.

### Background Checks

One very effective prevention measure is to use background checks for key employees. Although a background check is not a 100% effective means of identifying potential fraudsters and is not always cost effective for all employees, but it can reveal potential problems. A background check could disclose a criminal record and/or high debt. Either of these could be justifiable reasons for not hiring the person. High debt is evidence that the financial or economic pressure leg of the fraud triangle is already present. The criminal record shows the history of committing crimes before and readiness to commit a fraud.

The ACFE 2008 RTTN stated in a report that only 7% of fraud culprits in the study had previous criminal history, and only 12% had been previously terminated by an employer for fraud-related conduct. Another related measure, which is very simple but sometimes ignored, is calling the potential employee's references. There have been examples noted where simple phone call had a big influence on the appointment decision when a fraudster made a mistake in the references or confidently assumed that no one would check.

### Regular Audits

Regular audits can serve as an effective prevention measure and thus could increase the perception of detection. However, if the auditors use some effective audit tools and techniques to look for ongoing fraud aggressively, that would serve as a prevention measure. A key to the effectiveness of regular fraud audits is to identify, review, and analyse irregularities.

In some major financial frauds of recent years, the internal audit function was disabled and not allowed to do anything serious with financial information, but kept busy with other kinds of audits. The CEOs for those companies were taking no chances that some hard-working internal auditor might stumble onto their scams. That happened where one internal auditor came in late at night and secretly examined financial records to which she was not allowed access during the day by the senior executives. Eventually, she disclosed the financial fraud and exposed the fraudster CEO.

In another case, a small newspaper office in some university in USA had one accountant whose was responsible for doing all of the accounting. A retired accounting professor was responsible for regular audits of the newspaper accounts. In April of a certain year, the retired professor informed the university president that he was going to resign. He recommended that the president should find a replacement or shift it into some other place. The university, up until this time, did not have an internal audit function. In mid-October, the newspaper printing vendor representative called the university VP and said that his company would not print the next issue of the university newspaper because it had not been paid. The VP checked into the records and got to know that the accounting clerk had stolen thousands of dollars. Strangely enough, she began to steal in May of that year. Clearly the regular audit had served as a perception of detection measure for her, but once removed, she was able to rationalize the fraud.

### Internal Controls

Opportunity is basically an alternative expression for internal controls and is included in the fraud triangle. Of the three legs, the management can create a positively influencing environment for those aspects, though a fraud auditor or professional has little if any ability to affect rationalization or pressure. Pressure and rationalization aspects happen mostly in one's mind and can be difficult to observe directly. Specific control activities can restrict the chance to commit fraud and are more easily observed. Thus the control environment, specifically antifraud control activities, can act as preventive fraud measures. Historically, the most common mistake with regards to fraud in control activities is insufficient and unmonitored segregation of duties. Other internal controls include the following:

- Appropriate authorization procedures
- Satisfactory documentation, records, and audit trail
- Physical control of assets and records
- Independent checks on performance
- Monitoring of controls

### Invigilation

Invigilation is another form of surveillance. In invigilation, the fraud auditor creates a perfect environment that should be fraud-free. That is, it is a well-staffed and has a high profile fraud audit. Because the invigilation serves as a standard of what the entity should be earning in revenues, the employees will be very careful for not to commit fraudulent

activities during such a time. By analysing the revenues during the invigilation in comparison to other time periods, the fraud auditor can decide if frauds have been occurring regularly outside the invigilation.

Invigilation is mainly useful for undercover frauds for which normal detective methods are completely futile. Invigilation provides a benchmark to verify existing revenues and enables management to establish whether skimming or some other undercover scheme appears to have been carried out.

### Accounting Cycles

One way to manage prevention measures is to examine the accounting business processes in their natural cycles. Considering some of the common characteristics of frauds in these areas is a way to develop effective prevention measures.

### Generalizations

Accounting transactions and cycles are specific to any given organization and it should be noted how they are linked. The link and specificity may be because of the industry, strategy, capital structure, culture, organizational structure, and various other factors. In order to prevent or detect fraud it is important to understand the underlying processes and the situational environment. No frauds occur within an empty space.

In fraud control, one of the most important factors to be considered is organizational size. Assignment of duties is greatly influenced by the organizational size, a critical area to fraud prevention and detection. The type and amount of fraud committed is also influenced by the size. When we talk about control methods, large organizations are more complicated, and therefore more problematic to control in most aspects, but they also have more control resources to spend. The opposite is true for smaller organizations. However, this generalization is not always true. For example, preventive control can be easily detected when the organizational structure is much thinner and more tightly connected but segregation of duties is hard to implement in small organizations as a preventive control. Again, the critical point here is to understand the fraud environment factors and the organizational context.

Each organization's accounting transactions and cycles differ from another, but on some level they are the same. Only a few basic accounting cycles exist. Although fraudulent transactions are of different forms but their constituents are the same.

### Sales Cycle

Lapping is a common scheme in the sales cycle. A person cannot afford to take more than a day or so off work at a time to carry on a lapping scheme for an extended period of time. There are two possible preventive measures for lapping, which are given below:

(1) Enforced rotation of duties.

(2) Enforced taking of vacation.

Delegation of duties can help prevent frauds such as larceny and write-off schemes. In many cases a simple independent authorization step needs to be added to the business process.

### Purchases Cycle

The highest percentage of frauds in the purchases cycle revolves around fraudulent payments. One common fraud is a shell company. This fraud can be committed when a party adds dealers to the authorized list. Many fraud schemes could be blocked by delegation of duties which is often a simple independent authorization step. This measure is very helpful in preventing false refunds, check tampering and false voids. Both in prevention and detection controls, transactions with related parties should be carefully inspected as this situation is another common area for fraud in disbursements.

### Payroll Cycle

In this cycle, the most common scheme to be considered is ghost employees. Employees' addition to the authorized payroll file could be carried out by an independent party to prevent fraud. Another prevention method is to validate payroll against human resource records once in a while. A ghost employee will be in the payroll but not in the human resource file. Forced rotation of duties and vacations in the payroll manager area is also a good prevention measure. Attention to people in and associated with the organization is another critical point. The human resource department is always highly focused on hiring the right people, but people still commit fraud. An effective fraud prevention system can be achieved by a thorough hiring process.

### Fraud response

There are three basic phases of an antifraud programme:

1) Prevention
2) Detection
3) Response

The response phase is compulsory if a fraud is detected. If an entity wants to detect all frauds committed against it, it is necessary for the management to think about what its response would be before a fraud actually occurs. This phase should be the first or second to be performed for an antifraud programme in terms of planning and developing policies and procedures. A fraud risk assessment may precede this step.

## Fraud Policy

A suitable fraud policy should be established before developing an effective fraud response. This step should occur before the occurrence of fraud and before developing specifics in an antifraud programme. There are several reasons for this which will be discussed later. When

creating the fraud policy, there are several issues to consider. First of all, a proper description of fraud is important. For example, if an employee ‘‘borrowed’’ the employer’s digital camera to take pictures of her personal property and then used the entity’s computers to make an account at ebay.com, and used this account to sell her stuff during company time, should we call it a fraud? A judge or jury may struggle with the belief that it is a fraud. But if the entity is following the Association of Certified Fraud Examiners (ACFE) definition and policy of fraud, and if employee had signed a copy indicating her agreement to obey to that policy, there would be no doubt in a courtroom regarding that case.

Similarly, if an employee borrows heavy equipment (e.g., backhoe) for the weekend to do some private work because it is not being used until next Monday, the entity should determine whether it should be considered a fraud and carefully implement the fraud policy.

In describing fraud, the following issues should be considered:

- Every deceitful or fraudulent act.
- Violation of trustworthy duties.
- Misuse of funds, securities, supplies, or other entity assets.
- Unofficial use of the entity’s assets; such as equipment or computers for personal use.
- Misstatements in the management or reporting of money or financial transactions.
- Profiteering due to insider knowledge of entity activities.
- Revealing confidential and exclusive information to outside parties.
- Disclosing to other persons about confidential activities engaged in or considered by the entity.
- Taking or looking for anything valuable from contractors, dealers, or persons providing services or materials to the entity. Exception: Gifts less than £50 in value.
- Damage, removal, or incorrect use of records (paper or digital), furniture, fixtures, or equipment.
- Harmful activities against the entity’s computers, systems, or technologies.
- Any violation of a relevant unlawful act.
- Any related or similar irregularity.

Management should include strategies for handling detected or suspected irregularities in the entity’s policy. The policy should specify where, who, what, when reports of suspicion should be reported for tips, complaints, or whistle blowing. The policy should be clear about the maintenance of the secrecy of tipsters. There should be some policy established to handle those reports and to make important decisions about an investigation and its process.

An appropriate level of privacy should be maintained by the policy, especially the protection of the rights of innocent employees including informers and whistle-blowers, who might get accidentally become involved in an investigation.

### Fraud Response Team

After a formal structure has been developed on paper, the next step is to identify people, positions, or units to be accountable for the different procedures specified in the fraud policy. A ‘‘fraud policy decision” is a tool to assist this part of fraud response and has been provided by the ACFE.

### Fraud Response Team and SMEs

| |
|---|
| **Litigation/Legal:** prosecution, knowledge of potential and successful prosecutors, civil proceedings |
| **Lawful/HR:** legal termination of criminal, legitimate concerns in investigating an employee |
| **Forensic accounting/CFE:** fraud investigation, fraud/legitimate evidence, appropriate interviews |
| **Digital forensics:** data withdrawal for evidence |
| **Cyber forensics:** evidence inserted in IT, concealed in IT, prospective cyber sources of evidence |
| **Executive administration:** accomplish all important decisions of the procedure and sequel |
| **Internal audit:** support the investigation, evidence collecting, controls remediation |
| **Public relations:** avoid publicity, manage publicity, create public responses to fraud |

Table: 10.1

An SME (Subject Matter Expert) in forensic accounting and fraud investigation is essential for a team. There is a difference between a fraud audit and a financial audit. A financial auditor or internal auditor cannot audit for evidence and/or conduct a fraud investigation. The approach towards a fraud audit is completely different from a financial audit, and a CPA who is not experienced in fraud investigations, cannot conduct a fraud audit or investigation.

Obviously, the response team should have the executive management as part of the team. The key decisions of the investigation will have to be made by senior management, and should be followed with some therapeutic activities to prevent fraud from happening to the entity again. Providing strategic means to recover the financial loss and assignment of responsibility of that process is a key duty of the management. However, while making the decision of who represents executive management, the entity should take into account the reality that the fraud could be perpetrated by a member of executive management.

Of course, the team could find one person who can perform multiple functions. For example, internal legal counsel should be able to handle litigation and legal HR matters.

Also, the entity may find a person who is an SME in cyber and digital forensics, or IA and digital forensics. Risk management could be collapsed with executive management. Some entities do not have all of the units indicated but they still have a medium to provide a list of issues to review. It also exhibits the need for assignment of certain activities where appropriate.

### Retrieval

The recovery of financial losses due to a fraud is part of the response phase. The amount may be significant and difficult to recover. There is often little to recover from the fraudster, because in most cases, the criminal has spent or hidden all the money.

Recovery can be achieved through the following means:

- Business insurance/bonding
- Repayment agreements
- Civil judgments

Repayment agreements and civil judgments are subject to many factors that could impair the entity's ability to fully recover and are beyond the control of the entity. Thus, insurance or bonding of key employees is the most strategic and reliable recovery approach.

An appropriate insurance provider should be selected by the management. Some insurance companies require the client to turn over fraud investigation to the insurance company and its forensic accounting system. In this situation, the management loses the opportunity to pursue prosecution and civil proceedings, but can still work on termination of employees. Sometimes the obligation is paid off by the insurance company without any investigation.

Consequently, an insurance provider should be selected by the entity, which offers a good fit in terms of the management's intentions about fraud response and the amount of coverage. In terms of recovery, both adequate insurance policies and successful litigation proceedings should be included in a good response plan.

## Suggested Further Readings


- ✓ Michael R. Young; November 2013; Financial Fraud Prevention and Detection: Governance and Effective Practices
- ✓ Golden, T.W., Skalak, S., Clayton, M. (2006) A Guide to Forensic Accounting Investigation
- ✓ Albrecht, C.C., Albrecht, W. (2005) Fraud Examination
- ✓ Brown, A., Doig, A., Summers, G., Dobbs, L. (2004) Practically Fraud
- ✓ Singleton, T., et al (2006) Fraud Auditing and Forensic Accounting