

**Practice Advisory 1210.A2-1:  
Auditor's Responsibilities Relating to Fraud Risk Assessment, Prevention, and  
Detection**

**Interpretation of Standard 1210.A2 from the  
*International Standards for the  
Professional Practice of Internal Auditing***

***Related Standard***

1210.A2 -The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

***Nature of this practice advisory:*** *Internal auditors should consider the following suggestions related to fraud. This guidance is not intended to represent all the considerations necessary, but provides a recommended minimum level of knowledge about fraud and actions for implementation. The level of training and experience required by an internal audit department and individuals within the department will vary depending on their established roles, as well as on the advisory and professional services expected from the chief audit executive by management and the board. Therefore, greater involvement requires a greater level of proficiency.*

*This practice advisory should be read in conjunction with PA1210.A2-2, "Auditor's Responsibilities Relating to Fraud Investigation, Reporting, Resolution, and Communication."*

**WHAT IS FRAUD?**

Fraud encompasses a range of irregularities and illegal acts characterized by intentional deception or misrepresentation, which an individual knows to be false or does not believe to be true. Throughout this practice advisory, and in PA1210.A.2-2, the guidance may refer to certain actions as "fraud", which may also be legally defined and/or commonly known as corruption. Fraud is perpetrated by a person knowing that it could result in some unauthorized benefit to him or her, to the organization, or to another person, and can be perpetrated by persons outside and inside the organization.

1. Fraud perpetrated to the detriment of the organization is conducted generally for the direct or indirect benefit of an employee, outside individual, or another organization. Some examples are:
  - Acceptance of bribes or kickbacks.
  - Diversion to an employee or outsider of a potentially profitable transaction that would normally generate profits for the organization.
  - Embezzlement, as typified by the misappropriation of money or property, and falsification of financial records to cover up an act, thus making detection difficult.
  - Intentional concealment or misrepresentation of events, transactions, or data.
  - Claims submitted for services or goods not actually provided to the organization.
  - Intentional failure to act in circumstances where action is required by the company or by law.

- Unauthorized or illegal use of confidential or proprietary information.
  - Unauthorized or illegal manipulation of information technology networks or operating systems.
  - Theft.
2. Fraud designed to benefit the organization generally produces such benefit by exploiting an unfair or dishonest advantage that also may deceive an outside party. Perpetrators of such acts usually accrue an indirect personal benefit, such as management bonus payments or promotions. Examples of fraud designed to benefit the organization include:
- Improper payments, such as illegal political contributions, bribes, and kickbacks, as well as payoffs to government officials, intermediaries of government officials, customers, or suppliers.
  - Intentional and improper representation or valuation of transactions, assets, liabilities, and income, among others.
  - Intentional and improper transfer pricing (e.g., valuation of goods exchanged between related organizations). By purposely structuring pricing techniques improperly, management can improve their operating results to the detriment of the other organization.
  - Intentional and improper related-party activities in which one party receives some benefit not obtainable in an arm's-length transaction.
  - Intentional failure to record or disclose significant information accurately or completely, which may present an enhanced picture of the organization to outside parties.
  - Sale or assignment of fictitious or misrepresented assets.
  - Intentional failure to act in circumstances where action is required by the company or by law.
  - Intentional errors in tax compliance activities to reduce taxes owed.
  - Prohibited business activities, such as those that violate government statutes, rules, regulations, or contracts.

In addition to the above, different manners for classifying or categorizing fraud exist. The auditor may want to explore information published by professional accounting or fraud investigation firms and associations to determine which classification method is most appropriate for their organization.

## WHY DOES FRAUD OCCUR?

There are generally three factors that influence the commission of fraud. These are opportunity, motive, and rationalization.

### 1. **Opportunity**

- A process may be designed properly for typical conditions. However, a window of opportunity may arise for something to go wrong or creates circumstances for the control to fail.
- An opportunity for fraud may exist due to poor control design or lack of controls. For example, a system can be developed that appears to protect assets, but which is missing an important control. Anyone aware of the gap can take what they want without much effort.
- Persons in positions of authority can create opportunities to override existing controls, because subordinates or weak controls allow them to circumvent the rules.

### 2. **Motive** (also called incentive or pressure)

- While people can rationalize their acts, there needs to be a motive to make them behave that way.
- Power is a great motivator. Power can be simply gaining esteem in the eyes of family or coworkers. For instance, many computer frauds are done to show the hacker has the power to do it rather than to cause intentional harm.
- Another motivator is the gratification of a desire, such as greed, or an addiction.
- The third motivator is pressure, either from physical stresses or from outside parties.

### 3. **Rationalization**

- Most individuals consider themselves good persons, even if they occasionally do something bad. To convince themselves they are still good persons, they may rationalize or deny their acts. For example, these individuals might consider that they were entitled to the stolen item or that if executives break the rules, it must be alright for others to do so as well.
- Some people will do things that are defined as unacceptable behavior by the organization, yet are commonplace in their culture or were accepted by previous employers. As a result, these individuals will not comply with rules that don't make sense to them.
- Some people may have periods of financial difficulty in their lives, have succumbed to a costly addiction, or are facing other pressures. Consequently, they will rationalize that they are just borrowing the money and, when their lives improve, they will pay it back. Others may feel that stealing from a company is not bad, thereby depersonalizing the act.

Although auditors may not be able to know the exact motive or rationalization leading to fraud, they are expected to understand enough about internal controls to identify opportunities for fraud. Auditors also should understand fraud schemes and scenarios, as well as be aware of the signs that point to fraud and how to prevent them. Information available from The IIA and other professional associations or organizations should be reviewed to ensure that the auditor's knowledge is current.

## FRAUD AND MISCONDUCT RISK ASSESSMENT

All organizations are exposed to a degree of fraud risk in any process where human input is required. The degree to which an organization is exposed relates to the fraud risks inherent in the business, the extent to which effective internal controls are present either to prevent or detect fraud, and the honesty and integrity of those involved in the process.

Fraud risk is the probability that fraud will occur and the potential severity or consequences to the organization when it occurs. The probability of a fraudulent activity is based, typically, on how easy it is to commit fraud, the motivational factors leading to fraud, and the company's fraud history. Fraud management includes limiting or eliminating consequences, which is more than limiting or eliminating financial loss. For example, for some organizations, loss of reputation may have considerable impact on their ability to attract and retain skilled employees or customers for their products, as well as to obtain facilities and licenses necessary for the business' growth and sustainability.

To assess fraud risk, internal auditors should use the organization's enterprise risk management model if one is in use. Otherwise, auditors could use the following guidelines:

1. Understand the specific fraud schemes that could threaten the organization. Use a risk model to map and assess the organization's vulnerability to these fraud schemes, which covers all inherent risks to the organization. The risk model also should use consistent categories (i.e., there should be no overlap between risk areas) and be detailed enough for a risk assessment to identify and cover anticipated high-risk areas.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Enterprise Risk Management framework provides a useful model that includes sections on:

- **Event identification**, such as brainstorming activities, interviews, focus groups, surveys, industry research, and event inventories.
  - **Risk assessments** that include probabilities and consequences.
  - **Risk response strategies**, such as treating, transferring, tolerating, or terminating risk.
  - **Control activities**, such as linking risks to existing anti-fraud programs and control activities, and validating their effectiveness.
  - **Monitoring**, including audit plans and programs that consider residual fraud and risk due to misconduct.
2. When evaluating controls to prevent or reduce fraud risks to an organization, cost and benefit considerations should be made. The evaluation should consider whether fraud could be committed by an individual or requires collusion. In practice, 100 percent fraud prevention is neither possible nor cost effective. Considerations also should be made regarding the negative effects of unjustly suspecting employees or giving the appearance that employees are not trusted.

## ELEMENTS OF FRAUD PREVENTION OR DETERRENCE

Fraud prevention involves those actions taken to discourage the commission of fraud and limit fraud exposure when it occurs. The principal mechanism for preventing fraud is internal control. Primary responsibility for establishing and maintaining internal control should rest with management.

The following are some control elements of a fraud prevention program presented within the COSO control framework as an example. Each element would be a valid consideration, regardless of which control framework the auditor uses.

1. **Control environment.** Companies must establish an appropriate control environment that includes:
  - A code of conduct, ethics policy, or fraud policy to set the appropriate tone at the top.
  - Ethics and whistleblower hotline programs to report concerns.
  - Hiring and promotion guidelines and practices.
  - Oversight by the audit committee, board, or other oversight body.
  - Investigation of reported issues and remediation of confirmed violations.
2. **Fraud risk assessment.** Organizations should identify and assess fraud-related risks, including assessing the potential for fraudulent financial reporting, asset misappropriations, improper receipts and expenditures, or financial misconduct by management and others. Companies also should assess whether adequate segregation of duties exists.
3. **Control activities.** Companies should establish and implement effective control practices, including actions taken by management to identify, prevent, and mitigate fraudulent financial reporting or misuse of the organization's assets, as well as prevent override of controls by management. In addition, companies should establish an affirmation or certification process to confirm employee have read and understood corporate policies and are in compliance with them.
4. **Information and communication.** Companies must establish effective fraud-related information and communication practices, including documentation and dissemination of policies, guidance, and results; opportunities to discuss ethical dilemmas; communication channels; training for personnel; and considerations of the impact and use of technology for fraud deterrence, such as the use of continuous monitoring software.
5. **Monitoring.** Organizations should conduct ongoing and periodic performance assessments and identify the impact and use of computer technology for fraud deterrence.

## Internal Auditor's Role

Internal auditors are responsible for assisting companies prevent fraud by examining and evaluating the adequacy and effectiveness of their internal controls' system, commensurate with the extent of a potential exposure within the organization. When meeting their responsibilities, internal auditors should consider the following elements:

1. **Control environment.** Assess aspects of the control environment, conduct proactive fraud audits and investigations, communicate results of fraud audits, and provide support for remediation efforts. In some cases, internal auditors also may own the whistleblower hotline.
2. **Fraud risk assessment.** Evaluate management's fraud risk assessment, in particular, their processes for identifying, assessing, and testing potential fraud and misconduct schemes and scenarios, including those that could involve suppliers, contractors, and other parties.
3. **Control activities.** Assess the design and operating effectiveness of fraud-related controls; ensure that audit plans and programs address residual risk and incorporate fraud audits; evaluate the design of facilities from a fraud or theft perspective; and review proposed changes to laws, regulations, or systems, and their impacts on controls.
4. **Information and communication.** Assess the operating effectiveness of information and communication systems and practices, as well as provide support to fraud-related training initiatives.
5. **Monitoring.** Assess monitoring activities and related computer software; conduct investigations; support the audit committee's oversight related to control and fraud matters; support the development of fraud indicators; and hire and train employees so they can have the appropriate fraud audit or investigative experience.

## FRAUD DETECTION

Management and the internal audit activity have different roles with respect to fraud detection. Here is a description of each:

### Management's Role in Fraud Detection

Management is responsible for establishing and maintaining an effective control system at a reasonable cost. This includes designing some controls to indicate when other controls are not working effectively. Following up on these indicators may result in the determination that fraud may have occurred.

One example of a monitoring control is the establishment and communication of a hotline or similar system customers or employees can use to make complaints or identify concerns. Other monitoring and detection controls include:

- Installing alarm systems on facility doors and windows.
- Installing surveillance cameras.
- Designing edit checks into information systems.
- Performing inventory counts.
- Auditing.
- Reviewing and approving invoices and cost centre charges.
- Reconciling accounts.

## Internal Auditor's Role in Fraud Detection

To the degree that fraud may be present in activities covered in the normal course of audit work, internal auditors have a responsibility to exercise due professional care as specifically defined in Standard 1220 of the *International Standards for the Professional Practice of Internal Auditing* with respect to fraud detection.

However, most internal auditors are not expected to have knowledge equivalent to that of a person whose primary responsibility is detecting and investigating fraud. Also, audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

A well-designed internal control system should not be conducive to fraud. Tests conducted by auditors improve the likelihood that any existing fraud indicators will be detected and considered for further investigation.

In conducting engagements, the internal auditor's responsibilities for detecting fraud are to:

- Consider fraud risks in the assessment of control design and determination of audit steps to perform. While internal auditors are not expected to detect fraud and irregularities, internal auditors are expected to obtain reasonable assurance that business objectives for the process under review are being achieved and material control deficiencies – whether through simple error or intentional effort – are detected.
- Have sufficient knowledge of fraud to identify red flags indicating fraud may have been committed. This knowledge includes the characteristics of fraud, the techniques used to commit fraud, and the various fraud schemes and scenarios associated with the activities reviewed.
- Be alert to opportunities that could allow fraud, such as control weaknesses. If significant control weaknesses are detected, additional tests conducted by internal auditors should be directed at identifying other fraud indicators. Some examples of indicators are unauthorized transactions, sudden fluctuations in the volume or value of transactions, control overrides, unexplained pricing exceptions, and unusually large product losses. Internal auditors should recognize that the presence of more than one indicator at any one time increases the probability that fraud has occurred.
- Evaluate the indicators of fraud and decide whether any further action is necessary or whether an investigation should be recommended.
- Notify the appropriate authorities within the organization if a determination is made that fraud has occurred to recommend an investigation.