

IPPF – Practice Guide

INTERNAL AUDITING AND FRAUD

DECEMBER 2009

Table of Contents

Introduction	1
Executive Summary	2
Definition of Fraud	4
Fraud Awareness	5
A. Reasons for Fraud	5
B. Examples of Fraud	7
C. Potential Fraud Indicators	8
Typical Roles & Responsibilities for Fraud	10
Internal Audit Responsibilities During Audit Engagement	13
A. Conducting Audit Engagements	13
B. Internal Auditor Skepticism	13
C. Communicating With the Board	14
Fraud Risk Assessment	16
A. Identifying Relevant Fraud Risk Factors	16
B. Identifying Potential Fraud Schemes and Prioritizing Them Based on Risk	17
C. Mapping Existing Controls to Potential Fraud Schemes and Identifying Gaps	17
D. Testing Operating Effectiveness of Fraud Prevention and Detection Controls	17
E. Documenting and Reporting on the Fraud Risk Assessment	18
Fraud Prevention and Detection	19
A. Fraud Prevention	19
B. Fraud Training	20
C. Fraud Detection	21
Fraud Investigation	23
A. Investigation Process	23
B. Internal Auditing’s Role in Investigations	23
C. Conducting the Investigation	24
D. Reporting Fraud Investigations	25
E. Resolution of Fraud Incidents	26
F. Communications of Fraud Incidents	26
G. Analysis of Lessons Learned	27
Forming an Opinion on Internal Controls Related to Fraud	29
Appendix A – Reference Material	30
Appendix B – Questions To Consider	32
Appendix C – Fraud Risk Assessment Template	33

Introduction

The purpose of this Practice Guide is to increase the internal auditor's awareness of fraud and provide guidance on how to address fraud risks on internal audit engagements.

The International Professional Practices Framework (IPPF) outlines the following *International Standards for the Professional Practice of Internal Auditing (Standards)* pertaining to fraud and the internal auditor's role in detecting, preventing, and monitoring fraud risks and addressing those risks in audits and investigations.

IIA Standard 1200: Proficiency and Due Professional Care

1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

IIA Standard 1220: Due Professional Care

1220.A1 – Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Related complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or non-compliance.
- Cost of assurance in relation to potential benefits.

IIA Standard 2060: Reporting to Senior Management and the Board

The chief audit executive (CAE) must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

IIA Standard 2120: Risk Management

2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

IIA Standard 2210: Engagement Objectives

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

In addition, see Appendix A – Reference Material which lists IPPF Practice Advisories that discuss fraud.

Executive Summary

Fraud negatively impacts organizations in many ways including financial, reputation, psychological and social implications. According to various surveys, monetary losses from fraud are significant. However, the full cost of fraud is immeasurable in terms of time, productivity, and reputation including customer relationships. Depending on the severity of the loss, organizations can be irreparably harmed due to the financial impact of fraud activity. Therefore, it is important for organizations to have a strong fraud program that includes awareness, prevention, and detection programs, as well as a fraud risk assessment process to identify fraud risks within the organization.

Frauds can be committed by an employee at any level within an organization, as well as by those outside the organization. There are three common characteristics of most frauds:

- Pressure or incentive — the need the fraudster is trying to satisfy by committing the fraud.
- Opportunity — the fraudster's ability to commit the fraud.
- Rationalization — the fraudster's ability to justify the fraud in his or her mind.

An effective fraud management program includes:

- Company ethics policy — “tone at the top” from senior management.
- Fraud awareness — understanding the nature, causes, and characteristics of fraud.
- Fraud risk assessment — evaluating the risk of various types of fraud.

- Ongoing reviews — an internal audit activity that considers fraud risk in every audit and performs appropriate procedures based on fraud risk.
- Prevention and detection — efforts taken to reduce opportunities for fraud to occur and persuading individuals not to commit fraud because of the likelihood of detection and punishment.
- Investigation — procedures and resources to fully investigate and report a suspected fraud event.

An effective internal audit activity can be extremely helpful in addressing fraud. Although management and the board are ultimately responsible for fraud deterrence, internal auditors can assist management by determining whether the organization has adequate internal controls and fosters an adequate control environment.

There are various approaches that the CAE may use in considering fraud while conducting internal audit activities:

- Auditing management controls over fraud. This includes policies, awareness practices, tone at the top, board and senior management governance (the control environment), as well as related practices, such as risk assessment, assessing the adequacy of preventive and detected controls in managing fraud risk within organizational tolerances, incident management, investigations, and recovery practices. Internal auditing should allocate resources to fraud-related activities in line with the risk of fraud relative to other organizational risks.
- Auditing to detect likely fraud by testing high-risk processes, with the intention of looking for indicators of fraud, within the organization and with external business relationships. For example, testing payroll for phantom employees, or testing vendor invoices for overcharges, matching vendor addresses with employee addresses to

detect fictitious vendors, or reviewing databases for duplicate transactions.

- Considering fraud as part of every audit. For example, brainstorming about fraud risk, evaluating fraud controls, designing procedures that consider the fraud risk, or evaluating errors to determine whether they could be an indication of fraud. The cumulative results may provide perspective on whether management's awareness and risk management programs have been implemented effectively across the organization.
- Consulting assignments help management identify and assess risk and determine the adequacy of the control environment for process reviews, new business ventures, or IT applications. Facilitation of management's self-assessment is another example of evaluating fraud risk, ensuring controls are in place to mitigate those risks, and who is monitoring results.

This document will discuss fraud and provide general guidance to help internal auditors comply with professional *Standards*. To learn more about detecting and controlling fraud, see Appendix A — Reference Material.

Definition of Fraud

Fraud encompasses a wide range of irregularities and illegal acts characterized by intentional deception or misrepresentation. The Institute of Internal Auditors' (IIA's) IPPF defines *fraud* as:

“Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.”

Another definition of *fraud* from the publication “*Managing the Business Risk of Fraud: A Practical Guide*,” sponsored by The IIA, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners, states:

“Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.”

Frauds are characterized by intentional deception or misrepresentation. This practice guide may refer to certain actions as “fraud,” which may also be legally defined and/or commonly known as *corruption*.

Fraud Awareness

Increased levels of fraud, a heightened regulatory environment, and pointed questions from internal and external auditors and boards of directors have caused companies to increase vigilance in their efforts to address fraud. Even amidst a culture of heightened awareness, however, an organization may be the victim of fraud and yet be unaware of this reality. Fraudulent schemes are often ongoing crimes that can last for months or even years before detection, making it difficult to measure the losses associated with fraud. Many fraud schemes are not publicized or even detected, making it difficult to measure the losses associated with fraud. Fraud losses that are known and confirmed make clear that the cost is high. The true cost of fraud, however, is even higher than just the loss of money, given its impact on time, productivity, reputation, and customer relationships.

Corruption — the misuse of entrusted power for private gain — and fraud have adversely impacted numerous organizations. The high cost of corporate governance, associated fines, and penalties have been a direct result of corporate frauds. Business executives have been involved in litigation, and in extreme circumstances, faced jail sentences when their global operations were not in compliance with legal and regulatory requirements.

Fraud has negatively impacted organizations in different ways, including financial, reputational, psychological, and social. Organizations have been forced to cease operations due to the impact of financial and reputation damages, and the psychological and social effects have been especially devastating to the employees of the organizations. Victims of fraud also suffer mental and emotional harm and stress-related physical effects in addition to their financial losses. The victims have felt robbed of not only their money, but also their security, self-esteem, and dignity. The bottom line is that fraud left unchecked can be detrimental to any organization.

Fraud can range from minor employee theft and unproductive behavior to misappropriation of assets, fraudulent financial reporting, or Ponzi schemes used to defraud investors. However, the risk of fraud can be reduced through a combination of prevention, detection, and deterrence measures. Most fraudulent schemes can be avoided with basic internal controls and effective audits and oversight. Unfortunately, fraud can be difficult to detect because it often involves concealment through falsification of documents or collusion among members of management, employees, or third-parties.

A. Reasons for Fraud

Most frauds begin small and continue to grow as the scheme remains undetected. For example, perpetrators often view initial stealing as temporary borrowings that will be fixed before anyone notices the problem. The borrowing accelerates and the perpetrators take positions that are indefensible or develop a scheme for the concealment and attempt to avoid discovery. As the fraud continues to grow, hopefully, it will be detected by a fellow employee, management, or an internal or external auditor.

Perpetrators primarily exploit inadequate internal controls for their own gain, resulting in substantial damage to the organization. The typical fraudster is a male of middle age, employed by the organization for a number of years. He often works in the financial department and typically commits the deed on his own terms, driven by a desire for money and opportunity. Many studies indicate that most frauds are committed by members of management. Managers generally have access to confidential information, enabling them to override internal controls and inflict greater damage to the organization than lower level staff members. Fraud perpetrators tend to be in positions of trust, educated, heads of households, and members of community organizations who are motivated by a personal need and are able to rationalize their actions.

Without minimizing individualized circumstances of each fraudulent scheme, the following are three common characteristics of frauds.

- Pressure or incentive represents a need that an individual attempts to satisfy by committing fraud. Often, pressure comes from a significant financial need or problem. This may include the need to keep one's job or earn a bonus. In publicly traded companies, there may be pressure to meet or beat analysts' estimates. For example, a large bonus or other financial award can be earned based on meeting certain performance goals. The fraudster has a desire to maintain his or her position in the organization and to retain a certain standard of living to compete with perceived peers.
- Opportunity is the ability to commit fraud and not be detected. Since fraudsters do not want to be caught in their actions, they must believe that their activities will not be detected. Opportunity is created by weak internal controls, poor management, lack of board oversight, and/or through the use of one's position and authority to override controls. Failure to establish adequate procedures to detect fraudulent activity also increases the opportunities for fraud to occur. A process may be designed properly for typical conditions, however, a window of opportunity may arise creating circumstances for the control to fail. Persons in positions of authority may be able to create opportunities to override existing controls because subordinates or weak controls allow them to circumvent the established controls.
 - Opportunity often occurs because the fraudster knows what the auditor will do — the when, what, and how much of the auditor's procedures. For example, if the fraudster knows that the auditor always tests only large transactions in December, the fraudster can

commit the fraud on smaller transactions in other months.

- Rationalization is the ability for a person to justify a fraud, a crucial component in most frauds. Rationalization involves a person reconciling his/her behavior (e.g., stealing) with the commonly accepted notions of decency and trust. For example, the fraudster places himself or herself as the priority (self-centered), rather than the well-being of the organization or society as a whole. The person may believe committing fraud is justified in the context of saving a family member or loved one so he/she can pay for high medical bills. Other times, the person simply labels the theft as "borrowing," and intends to pay the stolen money back at a later time. 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, they can rationalize their behavior as the rules don't apply to them.
 - Management might reduce rationalization through its actions, for example, by implementing fair work and pay practices, equitable and consistent treatment of employees, and tone at the top (management modeling the behavior expected of employees).

Gaining insight into the motivations of a fraudster and recognizing the threat that exposes every organization are the first steps in establishing and implementing an effective and sustainable fraud risk management system. Of the three elements, opportunity is the one that organizations can influence the most. Organizations need procedures and internal controls that avoid putting employees in positions to commit fraud and that detect fraudulent activities if they occur.

Although internal auditors may not know the exact motive or rationalization leading to fraud, they need to identify opportunities for fraud. Internal auditors also need to understand fraud schemes and scenarios, as well as be aware of the signs that point to fraud and how to prevent it.

B. Examples of Fraud

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 or inside the organization. Some common fraud schemes include:

- Asset misappropriation involves stealing cash or assets (supplies, inventory, equipment, and information) from the organization. In many cases, the perpetrator tries to conceal the theft, usually by adjusting the records.
- Skimming occurs when cash is stolen from an organization before it is recorded on the organization's books and records. For example, an employee accepts payment from a customer, but does not record the sale.
- Disbursement fraud occurs when a person causes the organization to issue a payment for fictitious goods or services, inflated invoices, or invoices for personal purchases. For example, an employee can create a shell company and then bill the employer for nonexistent services. Other examples include fraudulent health care claims (billings for services not performed, unbundled billings instead of bundled billings), unemployment insurance claims by people who are working, or pension or social security claims for people who have died.
- Expense reimbursement fraud occurs when an employee is paid for fictitious or inflated expenses. For example, an employee submits a fraudulent expense report claiming reimbursement for personal travel, nonexistent meals, extra mileage, etc.
- Payroll fraud occurs when the fraudster causes the organization to issue a payment by making false claims for compensation. For example, an employee claims overtime for hours not worked or an employee adds ghost employees to the payroll and receives the paycheck.
- Financial statement fraud involves misrepresenting the financial statements, often by overstating assets or revenue or understating liabilities and expenses. Financial statement fraud is typically perpetrated by organization managers who seek to enhance the economic appearance of the organization. Members of management may benefit directly from the fraud by selling stock, receiving performance bonuses, or using the false report to conceal another fraud.
- Information misrepresentation involves providing false information, usually to those outside the organization. Most often this involves fraudulent financial statements, although falsifying information used as performance measures can also occur.
- Corruption is the misuse of entrusted power for private gain. Corruption includes bribery and other improper uses of power. Corruption is often an off-book fraud, meaning that there is little financial statement evidence available to prove that the crime occurred. Corrupt employees do not have to fraudulently change financial statements to cover up their crimes; they simply receive cash payments under the table. In most cases, these crimes are uncovered through tips or complaints from third-parties, often via a fraud hotline. Corruption often involves the purchasing function. Any employee

authorized to spend an organization's money is a possible candidate for corruption.

- Bribery is the offering, giving, receiving, or soliciting of anything of value to influence an outcome. Bribes may be offered to key employees or managers such as purchasing agents who have discretion in awarding business to vendors. In the typical case, a purchasing agent accepts kickbacks to favor an outside vendor in buying goods or services. The flip side of offering or receiving anything of value is demanding it as a condition of awarding business, termed economic extortion. Another example is a corrupt lending officer who demands a kickback in exchange for approving a loan. Those paying bribes tend to be commissioned salespeople or intermediaries for outside vendors.
- A conflict of interest occurs where an employee, manager, or executive of an organization has an undisclosed personal economic interest in a transaction that adversely affects the organization or the shareholders' interests.
- A diversion is an act to divert a potentially profitable transaction to an employee or outsider that would normally generate profits for the organization.
- Unauthorized or illegal use or theft of confidential or proprietary information to wrongly benefit someone.
- Related-party activity is a situation where one party receives some benefit not obtainable in a normal arm's length transaction.
- Tax evasion is intentional reporting of false information on a tax return to reduce taxes owed.

C. Potential Fraud Indicators

Fraudsters often display certain behaviors or characteristics that may serve as warning signs or red flags. For example, some perpetrators act unusually irritable, some suddenly start spending lavishly, and some become increasingly secretive about their activities. However, the presence of those symptoms does not in and of itself signify that a fraud is occurring or will occur in the future.

Red flags may relate to time, frequency, place, amount, or personality. Red flags include overrides of controls by management or officers, irregular or poorly explained management activities, consistently exceeding goals/objectives regardless of changing business conditions and/or competition, preponderance of non-routine transactions or journal entries, problems or delays in providing requested information, and significant or unusual changes in customers or suppliers. Red flags also include transactions that lack documentation or normal approval, employees or management hand-delivering checks, customer complaints about delivery, and poor IT access controls such as poor password controls.

Personal red flags include living beyond one's means; conveying dissatisfaction with the job to fellow employees; unusually close association with suppliers; severe personal financial losses; addiction to drugs, alcohol or gambling; change in personal circumstances; and developing outside business interests. In addition, there are fraudsters who consistently rationalize poor performance, perceive beating the system to be an intellectual challenge, provide unreliable communications and reports, and rarely take vacations or sick time (and when they are absent, no one performs their work).

These red flags are often indicators of misconduct, and an organization's management and internal auditors need to be trained to understand and identify the potential warning signs of fraudulent conduct. While none of these mean an employee is actually committing fraud, a combination

of these factors could indicate a need for inquiries and heightened audit attention.

Awareness of fraud schemes is developed through periodic assessment by management and internal auditors, training of employees, and frequent communication between management and employees.

Typical Roles/Responsibilities for Fraud Prevention/Detection

An oversight function is important to effectively prevent or deter fraud. Oversight can take many forms and can be performed by many within and outside the organization, under the overall oversight of the board of directors.

Board of Directors

The board of directors has responsibility for effective and responsible corporate fraud governance. The role of the board is to oversee and monitor management's actions to manage fraud risks. Specifically, the board evaluates management's identification of fraud risks, implementation of anti-fraud measures, and creation of the tone at the top. Since the board is the organization's highest authority, it is responsible for setting the tone for fraud risk management within an organization. The board can implement policies that encourage ethical behavior, including processes for employees, customers, and external business relationship (EBR) partners to report instances where those policies are violated. The board may monitor the organization's fraud risk management effectiveness by appointing one executive-level member of management to be responsible for coordinating fraud risk management and reporting to the board. To set the appropriate tone at the top, the board of directors needs proper governance. This encompasses all aspects of board governance, including independent board members who exercise control over board information, agenda, access to management and outside advisers, and who independently carry out the responsibilities of the nominating/governance, compensation, audit, and other committees.

Audit Committee

An audit committee of the board of directors is the independent eyes and ears of the investors and other

stakeholders. The committee's role is to evaluate management's identification of fraud risks and the implementation of anti-fraud measures, and to provide the tone at the top that fraud will not be accepted in any form. The audit committee hires external auditors to report on the financial statements of the organization and provide recommendations on internal control. The external auditors report to the audit committee and not to management.

The audit committee usually has oversight of the internal audit activity. IIA Standard 2060: Reporting to the Board and Senior Management states that "the CAE must report periodically to senior management and to the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board."

The audit committee is responsible for overseeing controls to prevent or detect management fraud. In this role, the audit committee is responsible for overseeing senior management's compliance with appropriate financial reporting and for preventing senior management override of controls or other inappropriate influence over the reporting process.

Management

Management is responsible for overseeing the activities of employees and typically does so by implementing and monitoring processes and internal controls. In addition, management assesses the vulnerability of the entity to fraudulent activity. Fraud can occur in any organization, but the degree and detail involved in the risk assessment may correspond with the size and complexity of the organization.

Management is responsible for establishing and maintaining an effective internal control system at a reasonable cost. In addition, management's discussions with

investigators and legal counsel play an important role in developing controls over the investigation process, including developing policies and procedures for effective fraud investigations and for handling the results of investigations, reporting, and communications.

Legal Counsel

The roles and responsibilities of the in-house counsel will often be governed by the laws of each jurisdiction. A lawyer generally acts in the best interest of the organization and also is required to preserve client confidences. The discovery of fraud can bring these two ethical duties into a potential conflict. When faced with constituents in an organization who intend to engage in fraud, a lawyer can urge reconsideration, advise the constituents to seek a separate legal opinion, or refer the matter to a higher authority within the organization. The in-house counsel may decide to resign upon learning about potential or ongoing fraud, especially if the counsel's work product is used to further the fraud. If counsel resigns, the general counsel or outside counsel can document the measures taken to notify the wrongdoing members of the organization of the illegality of their 1) intended or ongoing conduct, 2) the consequences of that conduct, and 3) the counsel's attempt to deter the conduct.

Internal Auditors

Internal auditors evaluate risks faced by their organizations based on audit plans with appropriate testing. Internal auditors need to be alert to the signs and possibilities of fraud within an organization. While external auditors focus on misstatements in the financial statements that are material, internal auditors are often in a better position to detect the symptoms that accompany fraud. Internal auditors usually have a continual presence in the organization that provides them with a better understanding of the organization and its control systems. Specifically, internal auditors can assist in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness

of internal controls. In addition, they may assist management in establishing effective fraud prevention measures by knowing the organization's strengths and weaknesses and providing consulting expertise.

The importance an organization attaches to its internal audit activity is an indication of the organization's commitment to effective internal control and fraud risk management. The internal auditor's roles in relation to fraud risk management could include initial or full investigation of suspected fraud, root cause analysis and control improvement recommendations, monitoring of a reporting/whistleblower hotline, and providing ethics training sessions. If assigned such duties, internal auditing has a responsibility to obtain sufficient skills and competencies, including knowledge of fraud schemes, investigation techniques, and laws.

Internal auditors may conduct proactive auditing to search for misappropriation of assets and information misrepresentation. This may include the use of computer-assisted audit techniques, including data mining, to detect particular types of fraud. Internal auditors also can employ analytical and other procedures to find unusual items and perform detailed analyses of high-risk accounts and transactions to identify potential fraud.

At the appropriate time when enough information has been obtained, the CAE should keep senior management and the audit committee informed of special investigations in-progress and completed.

External Auditors

The organization's external auditors have a responsibility to comply with professional standards and to plan and perform the audit of the organization's financial statements to obtain reasonable assurance about whether the financial statements are free of material misstatement and whether the misstatements were caused by error or fraud. Whenever the external auditor has determined there is evidence that

fraud may exist, the external auditor's professional standards typically require that the matter be brought to the attention of an appropriate level of management. The external auditor typically reports fraud involving senior management directly to those charged with governance (e.g., the audit committee).

Loss Prevention Manager

The loss prevention (LP) manager (or company security group) deals with areas of business risk such as crimes, disasters, accidents, and waste, which have the capabilities to cause business failure. As the organization's security expert, the LP manager is in an advantageous position to lead risk communications between other risk and line managers. By identifying and understanding potential and actual patterns within the business, the LP manager can provide valuable insights to management on judging the effectiveness of the organization's risk management processes. The LP manager usually works closely with internal auditors to identify areas of weak internal controls within the organization.

Fraud Investigators

Fraud investigators are usually responsible for the detection and investigation of fraud, and the recovery of assets. They also perform a role in fraud prevention. Senior management and the audit committee need to support the investigators to let all stakeholders know the business entity is ready to respond quickly and appropriately to fraud risks. The organizational alignment of a fraud investigation unit (FIU) can vary. If a FIU is based within a corporate security department, it may be beneficial for them to work closely with or be involved in internal audit activities so the FIU employees will have access to internal and independent auditor findings. Fraud investigators often work closely with legal counsel to bring legal action against the perpetrator. Communications between fraud investigators and the legal counsel are likely to be considered confidential (e.g., privileged) to enable free and

open dialogue. Also, a fraud investigator's work done at the direction of legal counsel may constitute protected attorney work product.

The lead investigator usually determines the knowledge, skills, and other competencies needed to carry out the investigation effectively and assigns competent and appropriate people to the team. This process could include assurance that there is no potential conflict of interest with those being investigated or with any other employees of the organization.

Other Employees

Every employee has a role to play in fighting fraud. Employees are the eyes and ears of the organization, and they should be empowered to maintain a workplace of integrity. Employees can report suspicions of fraud to an employee hotline, the internal audit department, or a member of management. To deter and detect fraud and abuse, many experts believe an employee hotline that is appropriately monitored is the single most cost-effective fraud detection and deterrence measure.

Internal Audit Responsibilities During Audit Engagement

To the degree that fraud may be present in activities covered in the normal course of audit work, the *Standards* state that internal auditors have the following responsibilities with respect to fraud detection:

- Due Professional Care (Standard 1220).
- Risk Management (Standard 2120).
- Engagement Objectives (Standard 2210).

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 help prevent or detect material fraud. Tests conducted by internal auditors improve the likelihood that important fraud indicators will be detected and considered for further testing.

A. Conducting Audit Engagements

In conducting audit engagements, the internal auditor should:

- Consider fraud risks in the assessment of internal control design and determination of audit steps to perform. Internal auditors are not expected to detect fraud, but 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. The consideration of fraud risks is documented in the workpapers, as well as linkage of fraud risks to specific audit work.

- 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 deficiencies. If significant control deficiencies are detected, additional tests conducted by internal auditors could be used to identify whether fraud has occurred.
- Evaluate whether management is actively retaining responsibility for oversight of the fraud risk management program, that timely and sufficient corrective measures have been taken with respect to any noted control deficiencies or weaknesses, and that the plan for monitoring the program continues to be adequate for the program's ongoing success.
- Evaluate the indicators of fraud and decide whether any further action is necessary or whether an investigation should be recommended.
- Recommend investigation when appropriate.

Appendix B includes some questions internal auditing may routinely consider in its evaluation of an ongoing fraud risk management program.

B. Internal Auditor Skepticism

Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. An objective, skeptical internal auditor neither assumes that management or employees are dishonest nor assume unquestioned honesty.

In all audit work, the exercise of professional skepticism is paramount. Inadequate professional skepticism

is frequently cited as a significant reason why material fraud has not been detected. Internal auditors play a critical role in the success or failure of fraud risk management. With their intimate knowledge of the workings of an entity, internal auditors are in a unique position to identify many of the indicators of fraud. When internal auditors act with skepticism and they focus on the effectiveness of internal controls, the likelihood that they will notice the common characteristics of fraud is increased, and they might uncover possible fraudulent activity if and where it exists.

To allow internal auditors to exercise skepticism, IIA Standard 1111: Direct Interaction with the Board states that the CAE must communicate and interact directly with the board. In addition, Standard 1120: Individual Objectivity states that internal auditors must have an impartial and unbiased attitude, which is consistent with exercising skepticism. The audit committee's oversight and support of the internal audit activity helps the internal auditor maintain independence and objectivity as well as keep an attitude of skepticism.

C. Communicating With the Board

The relationship between the CAE and the board of directors includes both reporting and oversight functions. Internal auditors, through the unique role they play, are well positioned to elevate the importance of fraud prevention and detection programs with management and the board. Staying aware of what is happening in their specific industry and organization will enhance internal auditors' ability to address fraud risks with the board.

In discussions with the board, the CAE may include:

- All fraud audits performed.
- The fraud risk assessment process.

- Fraud or conflicts of interest and results of monitoring programs concerning compliance with law, code of conduct, and/or ethics.
- The internal audit activity's organizational structure as it pertains to addressing fraud.
- Coordination of fraud audit activity with external auditors.
- Overall assessment of the organization's control environment.
- Productivity and budgetary measures of internal audit's fraud activities.
- Benchmarking comparisons of internal audit's fraud activities with other organizations.
- Role of internal audit in fraud investigations.

The CAE may have a different opinion from senior management and the board about the right time to inform them of serious issues including fraud. A solution for addressing this timing concern is for the CAE to have discussions with senior management and the board before issues arise concerning what they need to know, when they need to know it, and how the communication will be made. Conducting this discussion is evidence that the CAE is complying with IIA Standard 2060: Reporting to Senior Management and the Board. The following illustration depicts an example of a document that could be prepared to clarify the nature and timing of a CAE's communication with the board regarding fraud matters.

Sample Audit Committee Event Matrix			When Events Should be Reported to the Audit Committee			
	Event	Magnitude	Immediately	At Next Meeting	Annual Report	Annual Summary
1	Defalcations, fraud, theft:					
	Not involving senior management					
	Major control breakdown	More than \$10,000	X			
	Involving collusion	More than \$10,000		X		
	Minor	Under \$10,000				X
	Involving senior management	All	X			
2	Denial of IA access to people or data	All	X			
3	Violation of Ethics Policy					
	Senior management	All	X			
	Middle management	All		X		
4	Discussion of replacement of the CAE	All activity in advance	X			

Fraud Risk Assessment

All organizations are exposed to fraud risk in any process where human involvement is required. An organization's exposure to fraud is a function of 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 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 organization's fraud history.

A fraud risk assessment is often a critical component of an organization's larger enterprise risk management program. The fraud risk assessment is a tool that assists management and internal auditors in systematically identifying where and how fraud may occur and who may be in a position to commit fraud. A review of potential exposures represents an essential step in alleviating the board's and senior management's concerns about fraud risks and their ability to meet organizational goals while promoting public confidence in the health of an organization. A fraud risk assessment concentrates on fraud schemes and scenarios to determine the presence of internal controls and whether or not the controls can be circumvented.

An important role of management is to provide oversight for the successful completion of a fraud risk assessment so that management has a better understanding of fraud risks and the controls in place to mitigate those risks. Organizations will need to reach their own conclusions with respect to the cost of controlling a risk compared to the benefits of mitigating or eliminating that risk.

A fraud risk assessment generally includes five key steps:

1. Identify relevant fraud risk factors.
2. Identify potential fraud schemes and prioritize them based on risk.
3. Map existing controls to potential fraud schemes and identify gaps.
4. Test operating effectiveness of fraud prevention and detection controls.
5. Document and report the fraud risk assessment.

The scope of the fraud risk assessment may vary widely depending on the organization's size, complexity, or industry. For example, an online business that has few employees with limited inventory and little cash on hand would likely have different fraud risks than an organization with numerous physical locations and a large employee base with access to inventory and/or cash. One organization may complete an enterprisewide assessment and include all business areas in the assessment, while another organization may limit its focus to the most important business risk area. An organization with several subsidiaries may complete a separate assessment for each subsidiary or a combined assessment.

A. Identifying Relevant Fraud Risk Factors

The first step is to gather information about the organization's business activities to gain an understanding of fraud risks, including external business relationship partners. This process includes review of documentation of previous frauds and suspected frauds committed against or on behalf of the organization, evaluation of related frauds at similar organizations, and review of the organization's performance measures over the past few years compared with competitors. For example, inconsistent patterns between non-financial measures and financial measures, excessive

use of licensed software, and use of other's intellectual property may indicate possible fraud.

B. Identifying Potential Fraud Schemes and Prioritizing Them Based on Risk

Fraud, by definition, entails intentional misconduct designed to evade detection. As such, a fraud risk assessment team needs to engage in strategic reasoning to anticipate both the fraud scheme and the individuals within and outside the organization who could be in a position to perpetrate each scheme. A fraud risk assessment team is typically composed of individuals from the internal audit activity, finance, legal, IT, security, and potentially other functions depending on the nature of the organization.

The fraud risk assessment team identifies potential fraudulent schemes using brainstorming, management interviews, analytical procedures, and review of prior frauds. During this process, the fraud risk assessment team reviews the organization's activities, schemes relevant to the industry, geography, and programs, always considering the basic characteristics of fraud (pressure/incentive, opportunity, and rationalization), asking:

- Where are the opportunities for fraud?
- What is the level of pressure management is under that would lead it to override internal controls?
- Are there any consequences if management fails to reach goals?

Specific fraud areas should be identified without consideration of existing or effectiveness of internal controls (which is done later). The evaluation considers whether the fraud could be committed by an individual alone or requires collusion among employees or external persons.

The following factors are considered when prioritizing fraud risks:

- Monetary impact.
- Impact to the organization's reputation.
- Loss of productivity.
- Potential criminal/civil actions including potential regulatory noncompliance.
- Integrity and security over data.
- Loss of assets.
- Location and size of operations/units.
- Company culture.
- Management/employee turnover.
- Liquidity of assets.
- Volume and/or size of transactions.
- Outsourcing.

C. Mapping Existing Controls to Potential Fraud Schemes and Identifying Gaps

The fraud risk assessment team identifies preventive and detective controls in place to address each fraud risk and to assess the likelihood and significance of each potential fraud. Entity-level anti-fraud controls such as the existence of a whistleblower hotline and whistleblower protection policy, board oversight, results of continuous monitoring, code of conduct, and the tone of management's communications regarding their tolerance for fraud risk are important elements in this exercise. The risk of management's override of controls needs to be explicitly considered and the cost/benefit for controlling that risk should be evaluated.

D. Testing Operating Effectiveness of Fraud Prevention and Detection Controls

Internal auditing typically plays an important role in assessing the operating effectiveness of internal controls. Internal auditors consider not only the existence of the internal control, but also the effectiveness of the internal control through periodic testing of the control. For example, an organization may implement a security policy over network passwords, which requires passwords to be changed every 30 days; however, the network system

access controls do not block user access if the password is not changed as required. In this case, the internal control is present, but is not operationally effective.

E. Documenting and Reporting on the Fraud Risk Assessment

Organizations need to document the process that identifies and evaluates fraud risk. Key elements that would likely be documented in a fraud risk assessment for each significant business area include:

- The types of fraud that have some chance of occurring.
- The inherent risk of fraud considering the availability of liquid and saleable assets, organizational morale and employee turnover, the history of fraud and losses, and other specific business area indicators.
- The adequacy of existing anti-fraud programs, monitoring, and preventative controls.
- The potential gaps in the organization's fraud controls, including segregation of duties.
- The likelihood of a significant fraud occurring.
- The business impact/significance of a fraud.

According to IIA Standard 2060: Reporting to Senior Management and the Board, the CAE must report periodically to senior management and to the board significant risk exposures and control issues, including fraud risks. Management and the CAE update the board periodically on the status and results of the fraud risk assessment. These updates report on the effectiveness of existing anti-fraud programs, as well as remediation efforts pursued by management to address gaps identified during the assessment.

Refer to Appendix C for an example of a fraud risk assessment. This template can be adapted for an enterprisewide fraud risk assessment by including other major business areas/units within the framework.

Fraud Prevention and Detection

Fraud can occur at various levels in an organization; therefore, it is important to establish appropriate preventive and detective techniques. Although fraud prevention and detection are related concepts, they are not the same. Fraud prevention entails implementing policies and procedures, employee training, and management communication to educate employees about fraudulent activities. On the other hand, fraud detection entails activities and programs designed to identify fraud or misconduct that is occurring or has occurred. The interrelationship between fraud prevention, detection, and investigation is shown in the chart below.

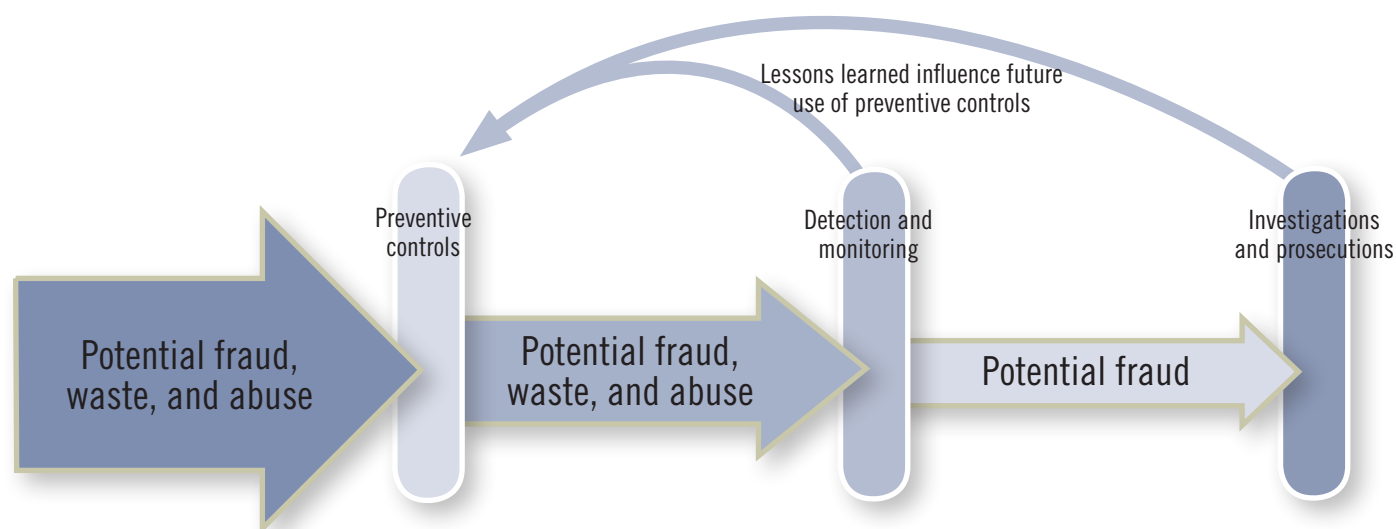
Organizations can never eliminate the risk of fraud. There are always people who are motivated to commit fraud, and an opportunity can arise for someone in any organization to override internal controls or to collude with others to circumvent internal controls. Although every organization is susceptible to fraud, it is not cost-effective to try to eliminate all fraud risk. An organization may choose to

design its controls to detect, rather than prevent fraud risks. If the cost of designing, implementing, and monitoring internal controls against fraud exceeds the estimated impact of the risk, it may not be cost-effective to implement the internal controls.

To understand and assess the opportunity for fraud to occur in an organization, one needs to gain an understanding of the corporate culture. Corporate culture provides a holistic and comprehensive view of the overall management philosophy and control environment. A strong ethical corporate culture alone will not protect an organization from fraud. While cultivating an ethical culture is a critical first step, reducing fraud risk also requires training and education, strong policies and procedures to implement and monitor internal controls, procedures to detect fraud risk indicators on a timely basis to investigate fraud, and prosecution when appropriate.

A. Fraud Prevention

Fraud prevention involves those actions taken to discourage the commission of fraud and limit fraud exposure when it occurs. Instilling a strong ethical culture and



setting the correct tone at the top are essential elements in preventing fraud. A strong principal mechanism for preventing fraud is effective and efficient internal controls, including controls related to screening customers, vendors, and external business relationship partners. An organization with effective internal controls deters fraudsters from the temptation to commit fraud. Management is primarily responsible for establishing and maintaining internal controls in an organization. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) presented a framework for assessing and improving internal control systems to fight fraud. COSO identified five components in its *Internal Control—Integrated Framework*: control environment, risk assessment, control activities, information and communication, and monitoring that may serve as the premise for the design of controls to fight fraud. The elements are deeply intertwined and overlapping in their nature and provide a natural interactive process to promote the type of environment in which fraud will not be tolerated at any level.

Control environment — Elements of a strong control environment help prevent fraud including the following:

- 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.

Risk assessment — Establishing a fraud risk assessment process that considers fraud risk factors and fraud schemes.

- Involving appropriate personnel in the fraud risk assessment process.

- Performing fraud risk assessments on a regular basis.

Control activities — Policies and procedures for business processes, including appropriate authority limits and segregation of incompatible duties.

Information and communication — Promoting the importance of the fraud risk management program and the organization's position on fraud risk both internally and externally through corporate communications programs.

- Designing and delivering fraud awareness training.
- An affirmation or certification process to confirm employees have read and understand corporate policies and that the employees are in compliance with the policies.

Monitoring — Providing periodic evaluation of anti-fraud controls.

- Using independent evaluations of the fraud risk management program by internal auditing or other groups.
- Implementing technology to aid in continuous monitoring and detection activities.

B. Fraud Training

Fraud training is usually a key factor in the deterrence of fraud. Training can cover the organization's expectations for employees' conduct, the procedures and standards necessary to implement internal controls, and employee roles and responsibilities to report misconduct. Employees need to understand the ethical behavior expected of them to act accordingly within the organization. New employee orientations can present the organization's mission, values and code of conduct, types of fraud, responsibility to report violations of ethical

behavior and impropriety, and details of the hotline or other ways to report potential fraud.

Employee fraud training needs to be tailored to the organization and the employee's position within the organization. Although generic fraud training can be helpful, it is more effective to identify the top fraud risk areas in the organization and develop training so that employees in key positions can better understand their role in the organization's fraud detection program. Fraudsters may even attend the training, which can benefit the organization, as they may be deterred by seeing the organization's fraud risk management process in action.

Periodic training throughout an employee's career reinforces fraud awareness and the cost of fraud to the organization. Regardless of the method used to produce and disseminate the training material, one key goal is to test the employee's comprehension of the fraud training. This can be done through online surveys that not only confirm attendance, but also offer quick exams to determine whether employees have gained the necessary knowledge from the training.

C. Fraud Detection

Detective controls are designed to provide warnings or evidence that fraud is occurring or has occurred. Effective internal controls are one of the strongest deterrents to fraudulent behavior and fraudulent actions. Simultaneous use of preventive and detective internal controls enhances any fraud risk management program's effectiveness. Although detective internal controls may provide evidence that fraud exists, detective internal controls are not intended to prevent fraud.

Fraud detection methods need to be flexible, adaptable, and continuously changing to meet the changes in the risk environment. While preventive measures are apparent and readily identifiable, detective controls may not be as apparent (i.e., they operate in the background).

Organizations often rely on employees to report suspicious activity through an anonymous whistleblower hotline. Using employee feedback capitalizes on the fact that many employees within the organization want to share what they know about organizational issues. An effective way for an organization to learn about existing fraud is to provide employees, suppliers, and other stakeholders with a variety of methods for reporting their concerns about illegal or unethical behavior. Ways to collect this information include:

- Code of conduct confirmation — When employees sign an annual code of conduct outlining their responsibilities in the prevention and detection of fraud, they can be asked to report any known violations.
- Whistleblower hotline — This can take the form of a telephone hotline or Web-based reporting system where the whistleblower can remain anonymous.
- Exit interviews — Conducting exit interviews of terminated employees or those who have resigned can help identify fraud schemes. They may also help determine whether there are issues regarding management's integrity, and may provide information regarding conditions conducive to fraud.
- Proactive employee survey — Routine employee surveys can be conducted to solicit employee knowledge of fraud and unethical behavior within the organization. A proactive survey could elicit anonymous information from employees, which would aid organizations in catching fraud sooner than if they wait for employees to volunteer such information.

All of these methods can use traditional telephone interviews, Web forms, e-mails, faxes, and face-to-face meetings.

Other methods for fraud detection include surprise audits in high fraud risk areas by either internal auditing, external

INTERNAL AUDITING AND FRAUD

auditing, or management; continuous monitoring of critical data and related trends to identify unusual situations or variances; and routine and/or ad hoc matching of public data and/or proprietary data against relevant transactions, vendor lists, employee rosters, and other data.

Fraud Investigation

Organizations investigate for possible fraud when there is a concern or suspicion of wrongdoing within the organization. Suspicions can result from a formal complaint process, informal complaint process such as tips, or an audit, including an audit designed to test for fraud. Investigating a fraud is not the same as auditing for fraud, which is an audit designed to proactively detect indications of fraud in those processes or transactions where analysis indicates the risk of fraud to be significant.

A fraud investigation consists of gathering sufficient information about specific details and performing those procedures necessary to determine whether fraud has occurred, the loss or exposures associated with the fraud, who was involved, and how it happened. An important outcome of investigations is that innocent persons are cleared of suspicion.

Investigations attempt to discover the full nature and extent of the fraudulent activity, not just the event that may have initiated the investigation. Investigation work includes preparing, documenting, and preserving evidence sufficient for potential legal proceedings.

Internal auditors, lawyers, investigators, security personnel, and other specialists from inside or outside the organization usually conduct or participate in fraud investigations.

Investigations and the related resolution activities need to be carefully managed in accordance with laws. Local laws may direct how and where investigations are conducted, disciplinary and recovery practices, and investigative communications. It is in the best interest of the company, both professionally and legally, to work effectively with the organization's legal counsel and to become familiar with the relevant laws in the country the fraud investigation occurs.

A. Investigation Process

Management is responsible for developing controls over the investigation process, including developing policies and procedures for effective investigations, preserving evidence, handling the results of investigations, reporting, and communications. Such standards are often documented in a fraud policy; internal auditors may assist in the evaluation of the policy. Such policies and procedures need to consider the rights of individuals, the qualification of those authorized to conduct investigations, and the relevant laws where the frauds occurred. The policies should also consider the extent to which management will discipline employees, suppliers, or customers, including taking legal measures to recover losses and civil or criminal prosecution. It is important for management to clearly define the authority and responsibilities of those involved in the investigation, especially the relationship between the investigator and legal counsel. It is also important for management to design and comply with procedures that minimize internal communications about an ongoing investigation, especially in the initial phases.

The policy needs to specify the investigator's role in determining whether a fraud has been committed. Either the investigator or management will decide if fraud has occurred and management will decide whether the organization will notify outside authorities. A judgment that fraud has occurred may in some jurisdictions be made only by law enforcement or judicial authorities. The investigation may simply result in a conclusion that organization policy was violated or that fraud is likely to have occurred.

B. Internal Auditing's Role in Investigations

The role of the internal audit activity in investigations needs to be defined in the internal audit charter, as well as in the fraud policies and procedures. For example, internal auditing may have the primary responsibility for fraud investigations, may act as a resource for investigations, or may refrain from involvement in investigations. Internal auditing

may refrain from involvement because it is responsible for assessing the effectiveness of investigations or it lacks the appropriate resources to be involved in investigations. Any of these roles can be acceptable as long as the impact of these activities on internal auditing's independence is recognized and handled appropriately.

To maintain proficiency, fraud investigation teams have a responsibility to obtain sufficient knowledge of fraudulent schemes, investigation techniques, and applicable laws. There are national and international programs that provide training and certification for investigators and forensic specialists.

If the internal audit activity is responsible for the investigation, it may conduct an investigation using in-house staff, outsourcing, or a combination of both. In some cases, internal auditing may also use nonaudit employees of the organization to assist. It is often important to assemble the investigation team without delay. If the organization is likely to need external experts, the CAE may pre-qualify the service provider[s] so external resources are quickly available when needed.

In organizations where primary responsibility for the investigation function is not assigned to the internal audit activity, the internal audit activity may still be asked to help gather information and make recommendations for internal control improvements.

C. Conducting the Investigation

An investigation plan is developed for each investigation, following the organization's investigation procedures or protocols. The lead investigator determines the knowledge, skills, and other competencies needed to carry out the investigation effectively and assigns competent, appropriate people to the team. This process includes obtaining assurance that there is no potential conflict of interest with those being investigated or with any of the employees in the organization.

The plan should consider the following investigative activities:

- Gathering evidence through surveillance, interviews, or written statements.
- Documenting and preserving evidence, considering legal rules of evidence, and the business uses of the evidence.
- Determining the extent of the fraud.
- Determining the techniques used to perpetrate the fraud.
- Evaluating the cause of the fraud.
- Identifying the perpetrators.

At any point during this process, the investigator may conclude that the complaint or suspicion was unfounded and then the investigator follows the organization's process to close the case.

The specific procedures employed in each investigation will differ based on the specific situation and the goals of the investigative team. The common investigative procedures include:

- **Obtaining evidence:** The collection and preparation of evidence is critical to understanding the fraud or misconduct, and it is needed to support the conclusions reached by the investigation team. The investigation team may use computer forensic procedures or computer-assisted data analysis based on the nature of the allegations, the results of the procedures performed, and the goals of the investigation. All reports, documents, and evidence obtained should be recorded chronologically in an inventory or log. Some examples of evidence include:

- Letters, memos, and correspondence, both in hard copy or electronic form (such as e-mails or information stored on personal computers).
 - Computer files, general ledger postings, or other financial or electronic records.
 - IT or system access records.
 - Security and time keeping logs, such as security camera videos or access badge records.
 - Internal phone records.
 - Customer or vendor information both in the public domain and maintained by the organization, such as contracts, invoices, and payment information.
 - Public records such as business registrations with government agencies or property records.
 - News articles, internal and external Web sites, such as social networking sites.
- **Interviewing:** The investigator will interview individuals such as witnesses and facilitating personnel. Typically, the accused individual is interviewed after most applicable evidence has been obtained. Many investigators prefer to approach the accused with sufficient evidence that will support the goal to secure a confession. Generally the accused is interviewed by two people: 1) an experienced investigator and 2) another individual who takes notes during the interview and later functions as a witness if needed. In addition, it is essential that all information obtained from the interview is rendered correctly.

Investigative activities need to be coordinated with management, legal counsel, and other specialists, such as human resources and insurance risk management, as appropriate throughout the investigation.

Investigators need to be knowledgeable and cognizant of the rights of persons within the scope of the investigation and the reputation of the organization itself. The investigator has responsibility to ensure that the investigation process is handled in a consistent and prudent manner.

The level and extent of complicity in the fraud throughout the organization needs to be assessed. This assessment can be critical to not destroying or tainting crucial evidence, and to avoid obtaining misleading information from persons who may be involved.

The investigation needs to adequately secure evidence collected, maintaining chain of custody procedures appropriate for the situation.

D. Reporting Fraud Investigations

Reporting fraud investigations consists of the various oral, written, interim, or final communications to senior management and/or the board regarding the status and results of fraud investigations. Reports can be preliminary and ongoing throughout the investigation.

A written report or other formal communication may be issued at the conclusion of the investigation phase. It may include the reason for beginning an investigation, time frames, observations, conclusions, resolution, and corrective action taken (or recommendations) to improve controls. Depending on how the investigation was resolved, the report may need to be written in a manner that provides confidentiality for some of the people involved. In writing the report, the investigator needs to consider the needs of the board and management while complying with legal requirements and restrictions, and the organization's policies and procedures.

Additional considerations concerning fraud reporting are:

- Submitting a draft of the proposed final communications on fraud to legal counsel for review. In cases where the organization is able to invoke attorney-client privilege, and has chosen to do so, the report is addressed to legal counsel.
- Notifying senior management and the board timely when significant fraud or erosion of trust occurs.
- The results of a fraud investigation may indicate that fraud had a previously undiscovered adverse effect on the organization's financial position and its operational results for one or more years for which financial statements have already been issued. Senior management and the board need to be informed of such a discovery so they can decide on the appropriate reporting, usually after consulting with the external auditors.

If internal auditing conducts the investigation, IIA Standard 2400: Communicating Results provides information applicable to necessary engagement communications.

E. Resolution of Fraud Incidents

Resolution consists of determining what actions will be taken by the organization once a fraud scheme and perpetrator[s] have been fully investigated, and evidence has been reviewed. Management and the board are responsible for resolving fraud incidents — not the internal audit activity or the investigator.

Resolution may include all or some of the following:

- Providing closure to persons who were initially under suspicion but were found to be innocent.
- Providing closure to those who reported a concern.

- Disciplining an employee in accordance with the organization's policies, employment legislation, or employment contracts.
- Requesting voluntary financial restitution from an employee, customer, or supplier.
- Terminating contracts with suppliers.
- Reporting the incident to law enforcement, regulatory bodies, or similar authorities; encouraging them to prosecute the fraudster; and cooperating with their investigation and prosecution.
- Entering into civil litigation or similar legal processes to recover the amount taken.
- Filing an insurance claim.
- Filing a complaint with the perpetrator's professional association.
- Recommending control enhancements.

F. Communications of Fraud Incidents

In addition to fraud reporting mentioned above, the two types of communications that may result from an investigation are public communications and planned internal communications.

Management or the board determines whether to inform entities outside the organization after consultation with individuals such as legal counsel, human resources personnel, and the CAE. The organization may have a responsibility to notify government agencies of certain types of fraudulent acts. These agencies include law enforcement, regulatory agencies, or oversight bodies. Additionally, the organization may be required to notify the organization's insurers, bankers, and external auditors of instances of fraud. Any comments made by management to the press, law enforcement,

or other external parties are best coordinated through legal counsel. Typically, only authorized spokespersons make external announcements and comments.

An important decision in this process is the decision to prosecute the wrongdoer. This decision is made by management and the board, usually based on the input of legal counsel. While internal auditors do not make these decisions, they may indicate to management and the board that prosecutions discourage future fraud by reinforcing the repercussions of fraudulent behavior and thus serve as a fraud deterrent.

Internal communications are a strategic tool used by management to reinforce its position relating to integrity, to demonstrate that it takes appropriate action (including prosecution if appropriate) when organization policy is violated, and to show why internal controls are important. Such communications may take the form of a newsletter article, a memo from management, or the situation may be used as an example in the organization's fraud training program. These communications generally take place after the case has been resolved internally, and they do not specify the names of perpetrators or other specific investigation details that are not necessary for the message or that contravene laws. An investigation and its results may cause significant stress or morale issues that may disrupt the organization, especially when the fraud becomes public. Management may plan employee sessions and/or team building strategies to rebuild trust and camaraderie among employees.

G. Analysis of Lessons Learned

After the fraud has been investigated and communicated, it is important for management and the internal audit activity to step back and consider the lessons learned. For example:

- How did the fraud occur?
- What controls failed?

- What controls were overridden?
- Why wasn't the fraud detected earlier?
- What red flags were missed by management?
- What red flags did internal audit miss?
- How can future frauds be prevented or more easily detected?
- What controls need strengthening?
- What internal audit plans and audit steps need to be enhanced?
- What additional training is needed?

Both management and internal auditors may hold lessons learned sessions. The dynamic feedback within these sessions needs to stress the importance of acquiring up-to-date information on fraudsters and fraud schemes that can help internal auditors and the anti-fraud community engage in best practices to prevent losses.

Management's fraud policies and procedures define who has authority and responsibility for each aspect of the process. The internal audit activity may be involved as advisers to the process, as long as the impact of these activities on internal auditing's independence is recognized and handled appropriately. In addition to advising management, internal auditors may become involved in investigations by:

- Monitoring the investigation process to help the organization follow relevant policies, procedures, and applicable laws and statutes (where internal auditing was not responsible for conducting the investigation).
- Locating and/or securing the misappropriated or related assets.
- Supporting the organization's legal proceedings, insurance claims, or other recovery actions.

INTERNAL AUDITING AND FRAUD

- Evaluating and monitoring the organization's internal and external post-investigation reporting and communication plans and practices.
- Monitoring the implementation of recommended control enhancement.

Internal auditors typically assess the facts of investigations and advise management relating to remediation of control weaknesses that lead to the fraud. Internal auditors may design steps in audit programs or develop “auditing for fraud” programs to help disclose the existence of similar frauds in the future.

Forming an Opinion on Internal Controls Related to Fraud

The internal auditor may be asked by management or the board to issue an opinion on the organization's system of internal controls related to fraud. See the following publications for more information on this topic:

- The IIA's Practice Advisories in the 2410 series.
- The IIA's Practice Guide, Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Controls.

Appendix A – Reference Material

The Institute of Internal Auditors (IIA), Practice Advisory 1210-1: Proficiency, www.theiia.org.

The IIA, Practice Advisory 1210.A1-1: Obtaining External Service Providers to Support or Complement the Internal Audit Activity, www.theiia.org.

The IIA, Practice Advisory 1220-1: Due Professional Care, www.theiia.org.

The IIA, Practice Advisory 2030-1: Resource Management, www.theiia.org.

The IIA, Practice Advisory 2060-1: Reporting to Senior Management and the Board, www.theiia.org.

The IIA, *Joining the Fight Against Corruption*, 2009, www.theiia.org.

The IIA, *The Role of Internal Auditing in Preventing and Detecting Misuse, Fraud, and Bribery*, Patty Miller, February 2007.

The IIA, *SOX Section 404: A Guide for Management by Internal Controls Practitioners*, second edition, The IIA, 2008, www.theiia.org.

The IIA Research Foundation, *Using Non-Financial Measures to Assess Fraud Risk*, Brazel, Jones, and Zimelman, August 2008, www.theiia.org.

Internal Auditor Magazine, “Fraud Risk Assessment,” Jonny Frank, April 2004, www.internalauditoronline.org.

Internal Auditor Magazine, “4 Steps to a Successful Fraud Risk Assessment,” Paul Zikmund, February 2008, www.internalauditoronline.org.

Internal Auditor Magazine, “The Risk Matrix Revisited,” Larry Hubbard, April 2009, www.internalauditoronline.org.

Internal Auditor Magazine, *Focusing on Fraud* issue, October 2009, www.internalauditoronline.org.

Public Accounting

American Institute of Certified Public Accountants (AICPA), “The Auditor’s Responsibility for Fraud and the Importance of Professional Skepticism,” 2008, www.aicpa.org.

Deloitte, *Fraud & the Regulatory Environment*, Stefan DuChene, March 2006, <https://www.tmaccalgary.com/presentation/Stefan%20DuChene.ppt>

KPMG LLP, *Profile of a Fraudster Survey 2007*, www.us.kpmg.com.

KPMG LLP, *Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response*, 2006, www.us.kpmg.com.

PricewaterhouseCoopers (PwC), *Internal Audit 2012: A Study Examining the Future of Internal Auditing and the Potential Decline of a Controls-centric Approach*, 2007, www.pwc.com.

Association Certified Fraud Examiners (ACFE)

The Association of Certified Fraud Examiners (ACFE)/ American Institute of Certified Public Accountants (AICPA), *Fraud Tools*, www.acfe.com.

ACFE, 2008 ACFE Report to the Nation on Occupational Fraud & Abuse, 2008, www.acfe.com.

ACFE, “How Fraud Hurts You and Your Government Organization,” <http://www.acfe.com/resources/fraud-tools.asp?copy=video>.

ACFE “Sample Fraud Policy,” http://www.acfe.com/documents/sample_fraud_policy.pdf.

Joint Papers

The IIA, ACFE, and AICPA, *Managing the Business Risk of Fraud: A Practical Guide*, 2008, www.theiia.org.

The IIA, ACFE, Information System Accountability and Control Auditors, Financial Executives Institute, Institute of Management Accountants, and Society of Human Resource Professionals, *Management Anti-Fraud Programs and Controls: Guidance to Help Prevent, Deter, and Detect Fraud*, 2002.

Miscellaneous

Howard Silverstone and Howard Davia, *Fraud 101: Techniques and Strategies for Prevention (Second Edition)*, 2005.

Appendix B – Questions To Consider

Conducting timely and appropriate discussions about fraud with all levels of the organization, including the audit committee, demonstrates the proactive role the internal audit activity is taking in this area. Some of the questions that internal auditors may ask about fraud on a regular basis include:

1. Does the organization have a fraud governance structure in place that assigns responsibilities for fraud investigations?
2. Does the organization have a fraud policy in place?
3. Has the organization identified laws and regulations relating to fraud in jurisdictions where it does business?
4. Does the organization's fraud management program include coordination with internal auditing?
5. Does the organization have a fraud hotline?
6. Does the audit charter describe internal auditing's roles and responsibilities relating to fraud?
7. Has responsibility for fraud detection, prevention, response, and awareness been assigned within the organization?
8. Do management and the CAE update the audit committee on fraud?
9. Does management promote fraud awareness and training within the organization?
10. Does management lead fraud risk assessments and include internal auditing in the assessment process?
11. Are the results of fraud risk assessments considered in the audit planning process?
12. Are periodic fraud awareness and training programs provided to all employees?
13. Are automated tools available to those responsible for preventing, detecting, and investigating fraud?
14. Has management identified the types of potential fraud risks in its areas of responsibility?
15. Do management and the CAE know where to obtain guidance on fraud from professional organizations?
16. Do management and internal auditors know their professional responsibilities relating to fraud?
17. Has management incorporated appropriate controls to prevent, detect, and investigate fraud?
18. Does management have the appropriate skill sets in place to perform fraud investigations?
19. Do management and the internal audit activity periodically assess the effectiveness and efficiency of fraud controls?
20. Are fraud investigation workpapers and supporting documents appropriately secured and retained?

Note: This list is not a checklist. It does not include all questions that may be needed to assess fraud risks in a given organization, nor contain necessary follow-up questions that depend on the answers to previous questions. Accordingly, auditors may use this as a start to create their own tools and to brainstorm fraud risks.

Appendix C – Fraud Risk Assessment Template

This table serves as an illustrative template of a fraud risk assessment. Customization or adjustment is needed to adapt it for your organization’s fraud risk assessment.

Owner	Fraud Risks	Controls	Monitoring	Likelihood	Impact
Construction Department	Collusion between contractor and subcontractor. <ul style="list-style-type: none"> • Bid rigging. • Bribes/kick-backs. 	<ul style="list-style-type: none"> • Qualify contractors prior to bidding (financial solvency, reputation). • Formal competitive bidding procedures are used when selecting a general contractor (GC). Example: Sealed Bids. • Subcontractor selection: For all work exceeding \$ limit, competitive bidding is required by GC. • Bid Confirmation Letters are sent to subcontractors to ensure integrity of bid process. • Perform background check that includes searching for past fraud or ethical violations. Also, have GC sign Ethics Statement. • Display fraud hotline number onsite. • Periodic internal audits are completed of selected projects to determine contract compliance and search for irregularities. 	<ul style="list-style-type: none"> • Construction Department • Procurement • Legal • Internal Auditing 	M	M

INTERNAL AUDITING AND FRAUD

Owner	Fraud Risks	Controls	Monitoring	Likelihood	Impact
Construction Department	<p>Design & build defects (inferior material used & construction not performed per specifications).</p> <ul style="list-style-type: none"> • Reputation risk (injury or fatality at site). 	<ul style="list-style-type: none"> • Execute construction contract with detailed scope of work (specifications). • Periodic site visitations by architects, local building inspectors, engineers, commission agents, and owner's construction representatives are made to ensure job is on schedule and built per specifications and code. • Display fraud hotline number onsite. • Periodic internal audits are completed of selected projects to determine contract compliance and search for irregularities. 	<ul style="list-style-type: none"> • Construction Department • Legal • Internal Auditing 	M	H

Owner	Fraud Risks	Controls	Monitoring	Likelihood	Impact
Construction Department	<p>Contractor over-billing:</p> <ul style="list-style-type: none"> • Price. • Quantity. • Duplicate charges. • Fictitious billings. • Purchase discounts not credited. • Related-party transactions. 	<ul style="list-style-type: none"> • Management reviews & approves invoices. • Cost tracking is performed to monitor each project's expenditures and determine reasons for significant variances from capital budget. • Research cost overruns thoroughly and obtain approval before adjusting contract price. • Any changes to scope of work include a written change estimate with management review and approval before work begins. • Owner's construction estimators review cost increases or credits for accuracy and competitiveness. • Contract states related party transaction or affiliates must be disclosed and approved by owner. Credit reports are obtained or Internet searches randomly performed. • Display fraud hotline number onsite. • Periodic internal audits are completed of selected projects to determine contract compliance and search for irregularities. 	<ul style="list-style-type: none"> • Construction Department • Capital Appropriation Committee • Legal • Estimator • Controllers • Internal Auditing 	M	M

INTERNAL AUDITING AND FRAUD

Owner	Fraud Risks	Controls	Monitoring	Likelihood	Impact
Construction Department	Failure to perform.	<ul style="list-style-type: none"> Signed & notarized Release of Contractor Lien is required before releasing funds to contractor. Procure Performance Bond in case contractor does not fulfill their contract obligations. A portion of the contractor's payment due (retainage) is not paid to contractor until 100 percent of work is completed and final contractor lien releases received. Display fraud hotline number onsite. Periodic internal audits are completed of selected projects to determine contract compliance and search for irregularities. 	<ul style="list-style-type: none"> Construction Department Controllers Internal Auditing 	M	L
Construction Department	Theft or diversion of materials/equipment from job site.	<ul style="list-style-type: none"> Owner assigns a project manager onsite to monitor job. The owner's onsite representative oversees procedures for controlling equipment and onsite materials. Hire onsite security guards. Display fraud hotline number onsite. Periodic internal audits are completed of selected projects to determine contract compliance and search for irregularities. 	<ul style="list-style-type: none"> Construction Department Internal Auditing 	H	L

Authors

- Gregory S. Dubis, CIA, CCSA, CISA, CFE
- Abraham D. Akresh CPA, CGFM
- Princy Jain: CIA, CCSA, CFE and CA (India)
- Lynn Morley, CIA, CGA
- Theresa M. Phipps, CPA
- Richard A. Schmidt, CPA, CIA, CFE

Reviewers and Contributors

- Douglas J. Anderson, CIA, CPA
- Steve Hunt, CIA, CISA, CGEIT, CBM
- Ken Askelson, CIA, CPA, CITP
- Rich Lanza, CPA, CFE, PMP
- Peter Millar
- Marilyn Prosch, Ph.D.
- Donald E. Sparks, CIA, CISA, ARM

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed process and procedures, such as tools and technique, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of the IIA's International Professional Practices Framework. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended and the guidance is endorsed by The IIA through formal review and approval process.

For other authoritative guidance materials provided by The IIA, please visit our Web site, www.theiia.org/guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

The copyright of this position paper is held by The IIA. For permission to reproduce, please contact The IIA at guidance@theiia.org.



GLOBAL HEADQUARTERS

247 Maitland Ave.
Altamonte Springs, FL 32701 USA

T: +1-407-937-1111
F: +1-407-937-1101
W: www.theiia.org