PLANNING AND CONDUCTING A FRAUD EXAMINATION

Why Conduct a Fraud Examination?

There are many reasons why organisations choose to conduct fraud examinations. In particular, a properly executed fraud examination can address a number of organisational objectives, including:

- Identifying improper conduct
- Identifying the persons responsible for improper conduct
- Stopping fraud
- Sending a message throughout the organisation that fraud will not be tolerated
- Determining the extent of potential liabilities or losses that might exist
- Helping to facilitate the recovery of losses
- Stopping future losses
- Mitigating other potential consequences
- Strengthening internal control weaknesses

In addition, in some instances, a fraud examination might be required by law. A duty to investigate can arise from statutes, regulations, contracts, or common law duties. For example, a corporation's directors and officers owe a common law duty of care to their organisation and shareholders, and therefore, when suspicions of fraud arise, it might be necessary for them to conduct an investigation to ensure that they have full knowledge of such issues affecting the company. Likewise, some laws hold employers accountable for investigating employee complaints involving certain matters, such as retaliation, discrimination, harassment, and similar issues.

What Fraud Examination Entails

The term *fraud examination* refers to a process of resolving allegations of fraud from inception to disposition, and it is the primary function of the anti-fraud professional. The fraud examination process encompasses a variety of tasks that might include:

- Obtaining evidence
- Reporting
- Testifying to findings
- Assisting in fraud detection and prevention

Obtaining Evidence

The value of a fraud examination rests on the credibility of the evidence obtained. Evidence of fraud usually takes the form of documents or statements by witnesses; therefore, fraud examiners must know how to properly and legally obtain documentary evidence and witness statements.

Reporting

Once evidence has been obtained and analysed, and findings have been drawn from it, the fraud examiner must report the results to the designated individuals (e.g., management, the board, or the audit committee). A fraud examination report is a narration of the fraud examiner's specific activities, findings, and, if appropriate, recommendations.

Such communications are necessary so that those responsible can determine the appropriate course of action.

The results of an examination can be communicated in various ways. The appropriate method of communication will depend on the facts at issue, but most reports are communicated orally or in writing.

When communicating the results of a fraud examination, the fraud examiner is responsible for providing clear, accurate, and unbiased reports reflecting the fraud examination results. This need arises from the possibility that such results might end up being read or used by various groups of people, such as organisation insiders, attorneys, defendants, plaintiffs, witnesses, juries, judges, the media, and so on.

Testifying to Findings

Often, fraud examiners are called upon to provide testimony and report their findings at a deposition, trial, or other legal proceeding. When providing testimony, fraud examiners must be truthful. They should also communicate in a clear and succinct manner.

Assisting in Fraud Detection and Prevention

Fraud examiners are not responsible for the prevention of fraud; such responsibilities belong to management or other appropriate authority. Nevertheless, fraud examiners are expected to actively pursue and recommend appropriate policies and procedures to prevent fraud.

Because of their education, experience, and training, Certified Fraud Examiners are uniquely qualified to assist organisations in the prevention and detection of fraud.

Fraud Examination and Forensic Accounting

Although fraud examination shares certain characteristics with forensic accounting, they are not the same discipline.

Forensic accounting is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation. The word *forensic* is defined by *Black's Law Dictionary* as "used in or suitable to courts of law or public debate." Therefore, *forensic accounting* is actually litigation support involving accounting.

Accordingly, most fraud examinations involve forensic accounting, but not all forensic accounting is fraud examination. For example, an individual hired to value the property in a minority shareholder derivative suit would engage in forensic accounting even if the engagement does not involve fraud.

While fraud examinations can be conducted by either accountants or nonaccountants, forensic accounting work can only be performed by accountants. In addition, while forensic accounting is litigation support work that involves accounting, fraud examinations only involve anti-fraud matters.

Most fraud examinations will generally fall under the category of forensic accounting because the majority of fraud examinations, investigations, and reports regarding fraud are done with "an eye towards litigation." This is because fraud examiners are taught to conduct fraud examinations with the assumption that they will end in litigation.

Forensic accounting can include many professional services. Typically, forensic accountants perform assignments involving:

- Computer forensics
- Electronic discovery
- Bankruptcies, insolvencies, and reorganisations
- Workplace fraud investigations
- Calculations of economic losses

- Business valuations
- Professional negligence

Fraud Examination Methodology

Fraud examination is a methodology of resolving signs or allegations of fraud from inception to disposition. The fraud examination methodology establishes a uniform, legal process for resolving signs or allegations of fraud on a timely basis. It provides that fraud examinations should move in a linear order, from the general to the specific, gradually focusing on the perpetrator through an analysis of evidence.

Fraud examinations involve efforts to resolve allegations or signs of fraud when the full facts are unknown or unclear; therefore, fraud examinations seek to obtain facts and evidence to help establish what happened, identify the responsible party, and provide recommendations where applicable.

When conducting a fraud examination to resolve signs or allegations of fraud, the fraud examiner should assume litigation will follow, act on predication, approach cases from two perspectives, move from the general to the specific, and use the fraud theory approach.

Assume Litigation Will Follow

Each fraud examination should begin with the proposition that the case will end in litigation. Thus, when a fraud examiner begins a fraud examination, he must assume that the case will end in litigation, and this assumption must be maintained and considered throughout the entire examination. If the fraud examiner assumes that litigation will occur, he will conduct the examination in accordance with the proper rules of evidence and remain well within the guidelines established by the legal systems.

Act on Predication

Fraud examinations must adhere to the law; therefore, fraud examiners should not conduct or continue fraud examinations without proper predication. *Predication* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe that a fraud has occurred, is occurring, and/or will occur. In other words, predication is the basis upon which an examination, and each step taken during the examination, is commenced.

A fraud examiner acts on predication when he has a sufficient basis and legitimate reason to take each step in an examination.

Accordingly, fraud examiners should begin fraud examination only when there are circumstances that suggest fraud has occurred, is occurring, and/or will occur, and they should not investigate beyond the available predication. If a fraud examiner cannot articulate a factual basis or good reason for an investigative step, he should not do it. Therefore, a fraud examiner should reevaluate the predication as the fraud examination proceeds. That is, as a fraud examination progresses and new information emerges, the fraud examiner should continually reevaluate whether there is adequate predication to take each additional step in the examination.

If a fraud examiner acts without predication, he might expose both himself and his client or employer to liability.

The requirement for predication, however, does not bar fraud examiners from accepting other forms of engagements in circumstances where predication is lacking. For example, a fraud examiner can conduct a fraud risk assessment for consulting purposes even if there is no reason to believe a fraud has occurred, is occurring, and/or will occur.

Approach from Two Perspectives

Fraud examiners should approach investigations into fraud matters from two perspectives: (1) by seeking to prove that fraud has occurred and (2) by seeking to prove that fraud has not occurred. To prove that a fraud *has* occurred, the fraud examiner must seek to prove that fraud has *not* occurred. The reverse is also true. To prove fraud *has not occurred*, the fraud examiner must seek to prove that fraud has occurred. The reasoning behind this two-perspective approach is that both sides of fraud must be examined because *under the law, proof of fraud must preclude any explanation other than guilt*.

Move from the General to the Specific

Fraud examinations commence when the full facts are unknown or unclear; therefore, they should proceed from the general to the specific. That is, fraud examinations should begin with general information that is known, starting at the periphery, and then move to the more specific details.

To illustrate, consider the order of interviews in fraud examinations. In most examinations, fraud examiners should start interviewing at the periphery of all possible interview candidates and move towards the witnesses who appear more involved in the matters that are the subject of the examination. Thus, the usual order of interviews is as follows:

- Neutral third-party witnesses, starting with the least knowledgeable and moving to those who are more knowledgeable about the matters at issue
- Parties suspected of complicity, starting with the least culpable and moving to the most culpable
- The primary suspect(s) of the examination

Use the Fraud Theory Approach

When conducting fraud examinations, fraud examiners should adhere to the fraud theory approach. The fraud theory approach is an investigative tool designed to help fraud examiners organise and direct examinations based on the information available at the time.

The fraud theory approach provides that, when conducting investigations into allegations or signs of fraud, the fraud examiner should make a hypothesis (or theory) of what might have occurred based on the known facts. Once the fraud examiner has created a hypothesis, he should test it through the acquisition of new information (or correcting and integrating known information) to determine whether the hypothesis is provable. If, after testing a hypothesis, the fraud examiner determines that it is not provable, he should continually revise and test his theory based on the known facts until it is provable, he concludes that no fraud is present, or he finds that the fraud cannot be proven.

Simply put, the fraud theory approach involves the following steps:

- Analysing available data
- Creating a hypothesis
- Testing the hypothesis
- Refining and amending the hypothesis

The following internal fraud case study illustrates the concepts involved in the fraud examination process. Although the case study is based on an actual incident, the names and certain other facts have been changed for purposes of illustration.

LINDA REED COLLINS CASE STUDY

Linda Reed Collins is purchasing manager for Bailey Books Incorporated in Ontario, Canada. Bailey, with $226 million in annual sales, is one of the country's leading producers of textbooks for the college and university market, as well as technical manuals for the medical and dental professions.

Bailey's headquarters consists of 126 employees, plus numerous sales personnel in the field. Because of the competitive nature of the textbook business, the company's profit margins are quite thin. Bailey's purchases average about $75 million annually, consisting mostly of paper stock and covering used in the manufacturing process. The great majority of the manufacturing is done in Mexico through contracts with the Mexican government.

The purchasing function is principally handled by three purchasing agents. Linda Reed Collins is the purchasing manager and has two other buyers who report to her, plus another 18 clerical and support personnel.

Because Bailey Books is required by investors and lenders to have audited annual financial statements, Bailey employs a large regional CPA firm to conduct its annual audit and has a staff of five internal auditors.

All internal fraud matters within Bailey are referred to Loren D. Bridges, a Certified Fraud Examiner. Often, internal fraud issues at Bailey involve defalcations by Bailey's cashiers, but Bridges also receives a constant stream of complaints alleging misconduct by Bailey Books' salespeople and distributors.

On January 28, Bridges received a telephone call in which the caller, who was male, wanted to keep his identity hidden. The caller, however, claimed to have been a "long-term" supplier of books, sundries, and magazines to Bailey. The caller said that ever since Linda Collins took over as purchasing manager for Bailey several years ago, he has been systematically "squeezed out" of doing business with Bailey. Although Bridges queried the caller for additional information, the caller hung up the telephone.

Under the facts in this case study, there could be many legitimate reasons why a supplier to Bailey would feel unfairly treated. Linda Reed Collins could be engaged in fraud, as the caller claimed, or the caller could be someone who has a personal vendetta against Collins and wants to get her fired. That is, Bridges does not have enough information to know if the

caller was "squeezed out" of doing business with Bailey or why this might have been the case. Because Bridges does not have all of the facts, he should investigate the matter using the fraud theory approach.

Analysing Available Data

Under the fraud theory approach, Bridges should begin by analysing the available data so he can create a preliminary hypothesis as to what has occurred.

Also, if those responsible determined that an audit of the entire purchasing function is warranted, the audit would be conducted at the time this determination is made. When conducting the audit, the internal auditors should keep in mind that there is a possibility that fraud might exist.

Creating a Hypothesis

Once Bridges has analysed the available data, he should create a preliminary hypothesis as to what has occurred. The hypothesis should be a "worst-case" scenario. That is, based on the caller's statements, Bridges should determine the worst possible outcome. Under these facts, the worst possible outcome would be that one of Bailey's purchasing agents has been accepting kickbacks to steer business to a particular vendor.

Fraud examiners can create hypotheses for any specific allegation (e.g., a bribery or kickback scheme, embezzlement, conflict of interest, or financial statement fraud).

Testing the Hypothesis

Once Bridges has created a hypothesis, he should test it through the acquisition of new information or by correcting and integrating known information.

Testing a hypothesis involves creating a "what-if" scenario. For example, in the facts of the Linda Reed Collins case study, Bridges hypothesises that, based on the anonymous tip, a vendor is bribing a purchasing agent. He would test this hypothesis by looking for some or all of the following facts:

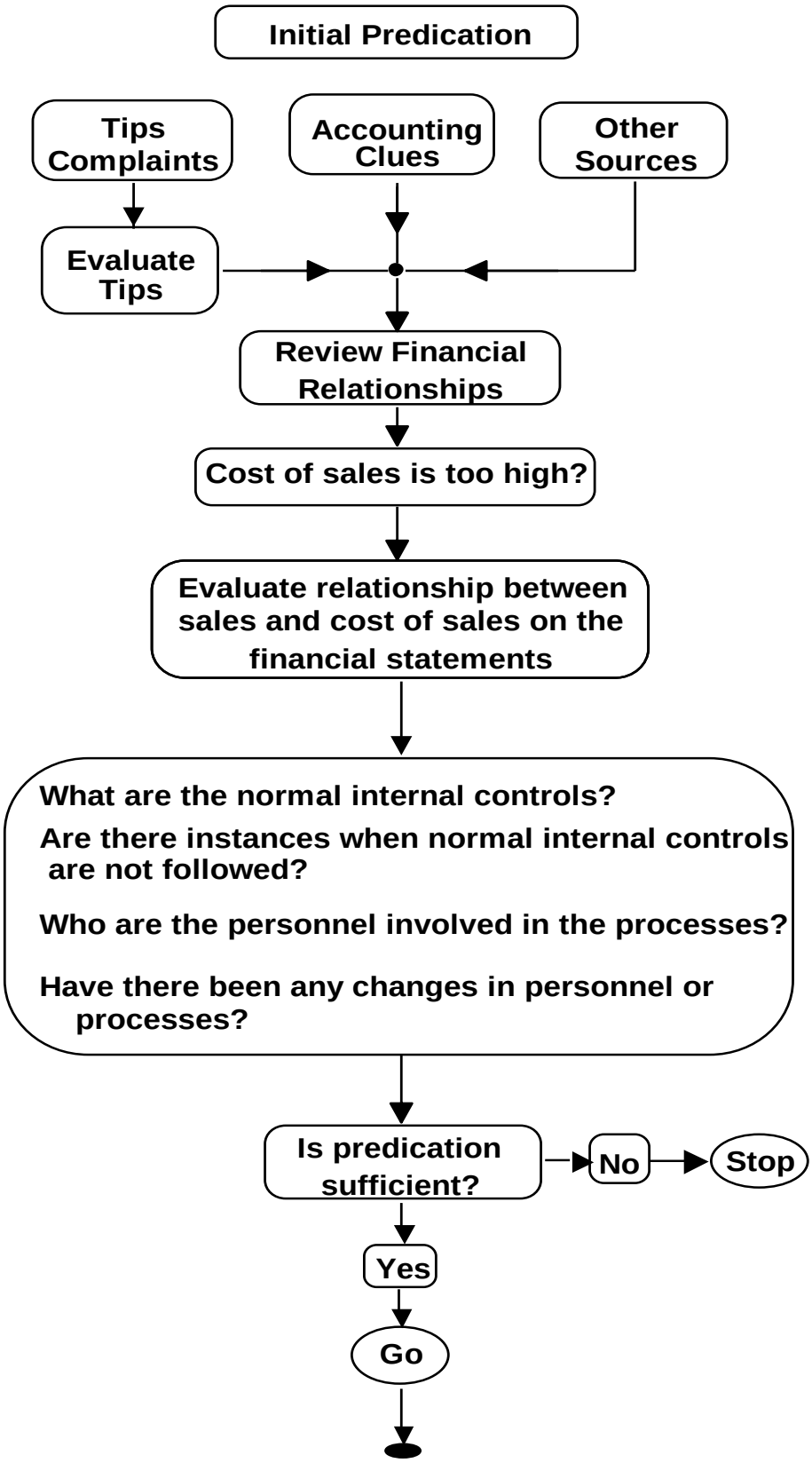
- A vendor is receiving an unusually large amount of business
- Purchases of high-priced, low quality goods or services over an extended period
- A purchasing agent has a personal relationship with a vendor
- A purchasing agent with the ability to steer business towards a favoured vendor
- A purchasing agent's lifestyle suggests unexplained wealth or outside income

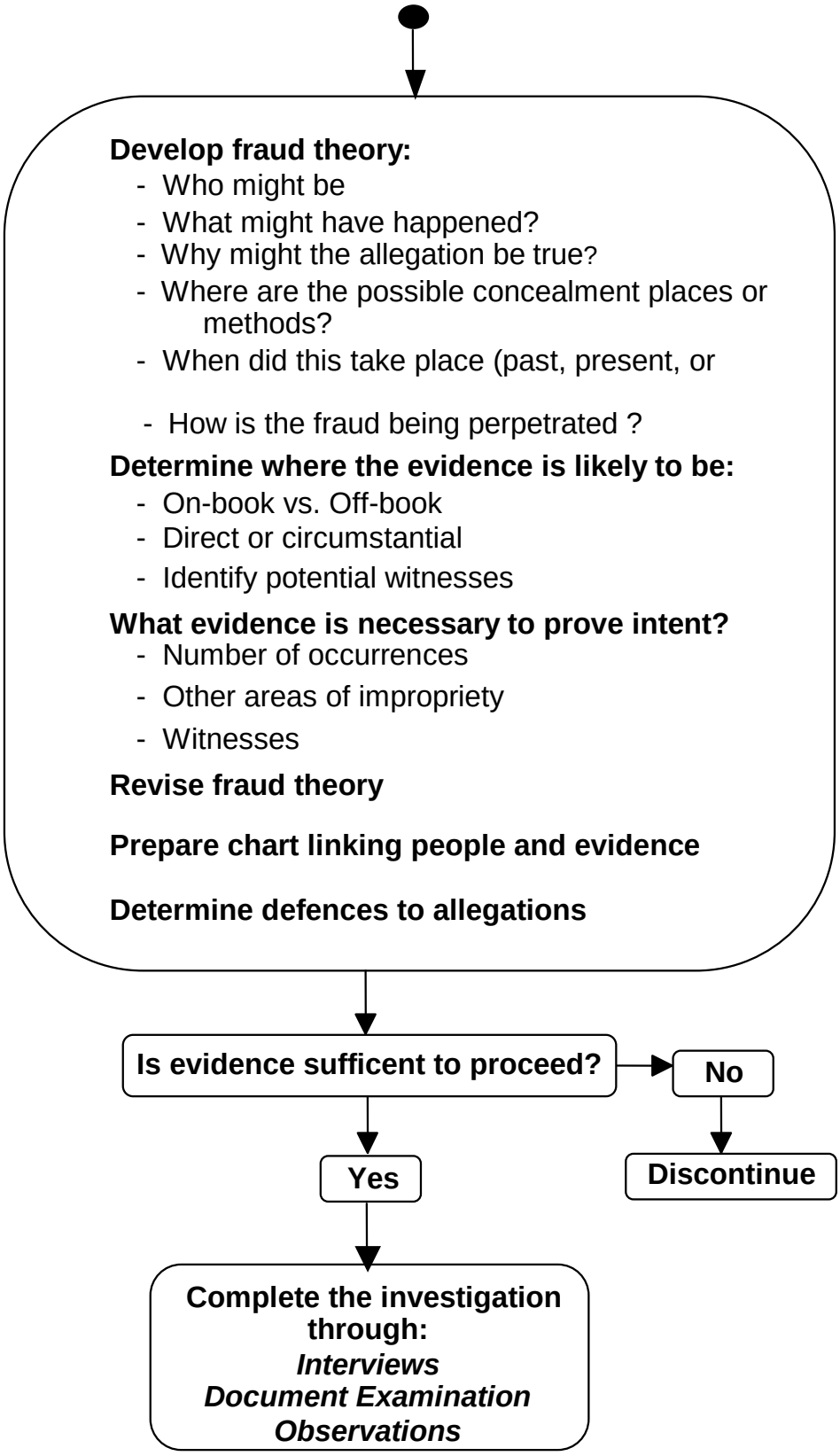
Bridges could readily look for facts indicating a bribery scheme. He could readily establish whether a vendor is receiving an unreasonably large proportion of Bailey Book's business when compared to similar vendors. Bridges could ascertain whether Bailey Books was paying too much for a particular product, such as paper, by simply calling other vendors and determining competitive pricing. Bridges could determine whether a vendor has a personal relationship with a purchasing agent by discreet observation or inquiry. Bridges could determine whether a particular purchasing agent had the ability to steer business towards a favoured vendor by determining who is involved in the decision making process. Also, Bridges could learn about the agent's lifestyle by examining public documents such as real estate records and vehicle titles.

Refining and Amending the Hypothesis

If, after testing a hypothesis, the fraud examiner determines that it is not provable, the fraud examiner should continually revise and test it based on the known facts. For example, if Bridges tests his hypothesis that a vendor is bribing a purchasing agent of Bailey Books and learns that the facts do not fit the presence of a bribery scheme, he should revise his hypothesis and retest it. (Obviously, if the fraud examiner tests his hypothesis and determines that the facts do not fit the presence of a bribery scheme, it could be that no fraud is present or that the fraud cannot be proven.)

The following flow chart sets forth how the fraud examination process is used to resolve signs or allegations of fraud.


Initial Predication
Tips Complaints
Accounting Clues
Other Sources
Evaluate Tips
Review Financial Relationships
Cost of sales is too high?
Evaluate relationship between sales and cost of sales on the financial statements
What are the normal internal controls?
Are there instances when normal internal controls are not followed?
Who are the personnel involved in the processes?
Have there been any changes in personnel or processes?
Is predication sufficient?
No
Stop
Yes
Go


Develop fraud theory:
- Who might be
- What might have happened?
- Why might the allegation be true?
- Where are the possible concealment places or methods?
- When did this take place (past, present, or
- How is the fraud being perpetrated ?
Determine where the evidence is likely to be:
- On-book vs. Off-book
- Direct or circumstantial
- Identify potential witnesses
What evidence is necessary to prove intent?
- Number of occurrences
- Other areas of impropriety
- Witnesses
Revise fraud theory
Prepare chart linking people and evidence
Determine defences to allegations
Is evidence sufficent to proceed?
No
Discontinue
Yes
Complete the investigation through:
Interviews
Document Examination
Observations

Develop a Fraud Response Plan

When evidence of misconduct arises, management must respond in an appropriate and timely manner. During the initial response, time is critical. To help ensure that an organisation responds to suspicious fraud-related activity efficiently, management should have a response plan in place that outlines how to respond to such issues.

A *fraud response plan* outlines the actions that members of an organisation will take when suspicions of fraud have arisen. Because every fraud is different, the response plan should not outline how a fraud examination should be conducted. Instead, response plans should help organisations manage their responses and create environments to minimise risk and maximise the potential for success.

Additionally, a response plan will allow management to respond to suspected and detected incidents of fraud in a consistent and comprehensive manner. By having a response plan in place, management will send a message that it takes fraud seriously.

More specifically, the fraud response plan should guide the necessary action when potential fraud is reported or identified.

Also, a response plan should not be unduly complicated; for a response plan to work in high-pressure and time-sensitive situations, it must be simple to understand and administer.

While the appropriate response will vary based on the event, management should include a range of scenarios in the response plan.

Organisations without a fraud response plan might not be able to respond to issues properly, and will likely expend more resources and suffer greater harm than those that have such a plan in place. Conversely, having a response plan puts an organisation in the best position to respond promptly and effectively.

This section explores the elements of a fraud response plan, which include:

- Reporting protocols
- A response team responsible for conducting an initial assessment
- Factors used to decide on the course of action
- Litigation hold procedures

- Principles for documenting the response plan
- A template or form to report fraud incidents

Reporting Protocols

One of the first steps when developing a response plan is to establish reporting protocols for tips, matters, allegations, and other indicators of improper activity. Reporting protocols are necessary to ensure that designated individuals are notified immediately to enable a prompt response.

Reporting protocols should outline notification principles and escalation triggers that vary depending on the nature and severity of the allegations. That is, they should indicate how to communicate the incidents to the appropriate level of management. For example, a fraud response plan might instruct employees to report suspicions of fraud to their manager (if possible), a designated human resources (HR) or compliance officer, or the head of audit and enforcement.

Next, the issue should be reported to the party or parties responsible for conducting an initial assessment to determine how to respond and whether a full investigation is necessary.

Additionally, organisations should provide multiple channels for reporting concerns about fraud.

A Response Team

No single person can effectively address every fraud-related issue. Therefore, the fraud response plan must identify key individuals who might be required to respond to a particular fraud. The response team members will vary depending on the facts and the potential severity of the suspected fraud, but the team might include:

- Legal counsel
- A representative of management
- A Certified Fraud Examiner
- The finance director
- General counsel
- A representative of internal audit
- Audit committee members
- A C-level executive

- Information technology (IT) personnel
- A representative of human resources (HR)

Factors Used to Decide on the Course of Action

Again, the response team should determine the appropriate course of action when fraud is suspected. In general, if an allegation of fraud-related misconduct arises, management should conduct an investigation, but there are other courses of action it might decide to take. To help decide the best course of action, management should identify a list of factors it will use to make this decision. Identifying such factors will help the response team determine whether to escalate an incident into an investigation.

Each organisation will have different criteria for deciding whether allegations/suspicions qualify for a formal investigation, but common ones include:

- Credibility of the allegation
- Type of incident
- The subject of the allegation
- The business purpose of the activity at issue
- Seriousness or severity of the allegation
- Potential negative impact
- Likelihood that the incident will end up in court
- The ways in which prior, similar incidents were handled

Litigation Hold Procedures

If an organisation does not already have litigation hold procedures in place, management should institute them immediately. A *litigation hold* refers to the steps an organisation takes to notify employees to suspend the destruction of potentially relevant records when the duty to preserve information arises.

Litigation hold procedures are necessary to ensure that potentially responsive documents are not destroyed once evidence of misconduct arises. The failure to preserve relevant evidence could have several adverse consequences, including, but not limited to, the government's questioning of the integrity of any fraud investigation, monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defences.

To establish litigation hold procedures, management should:

- Identify the scope of litigation hold procedures (i.e., the locations that the litigation hold procedures will cover).
- Examine how information moves through the organisation.
- Determine how to identify relevant documents.
- Develop a process to ensure such information is preserved.

Litigation hold procedures should apply to individual communications (e.g., email, chat messages, voice recordings), data on shared devices (e.g., network folders), system backup files, and archived data.

In general, litigation hold policies should be developed so the organisation can:

- Promptly notify employees who might possess relevant documents.
- Issue a preliminary hold order to all individuals and employees who might possess relevant information.
- Promptly notify information technology (IT) personnel and get their involvement if electronic data is at issue.
- Notify employees and IT personnel of their duty to preserve.
- Suspend any deletion protocols.
- Prohibit the destruction, loss, or alteration of any potentially relevant documents.
- Prohibit employees from destroying, hiding, or manipulating documents.
- Alert employees as to the risk to the company and the employees if they fail to heed the litigation hold request.

Moreover, establishing litigation hold procedures will help those involved in an investigation identify the relevant sources of information quickly, and it will help them understand the technology options available for searching, analysing, and reviewing data.

Even though litigation holds should apply to both electronic data and physical documents, electronic data contains certain attributes that make executing a timely litigation hold more difficult. Specifically, electronic data might only be available for a temporary period, business practices are often designed to free up storage space by deleting this type of information, electronic data can reside in numerous locations, and identifying relevant electronic data within today's large and complex data systems can be challenging and costly.

Moreover, if an organisation operates internationally, it is more difficult to execute a timely hold. In such cases, management should consider retaining an outside expert to help with the data search and preservation.

A key objective of a litigation hold is to stop any automatic document deletion programmes or rules that might be in place.

Principles for Documenting the Response Plan

Management should establish principles for documenting information during each phase of a fraud investigation. The principles should be designed to record all information relevant to or created during each phase of a fraud investigation, including the initial response, that is used to support decision making.

A Fraud Incident Report Log

Management should also develop a fraud incident report log of all suspicions of fraud, including those not investigated, to serve as a record of the organisation's response efforts. Once a suspicion of fraud arises, the issue should be recorded and detailed in the log, and as the issue progresses, the log should be modified. Ultimately, it should contain details of actions taken and conclusions reached.

The report log should include information on the following items:

- How the organisation became aware of the suspected fraud, including the name of any complaining party
- The date the issue was raised or reported
- The nature of the suspected fraud
- Department or divisions involved
- Suspect employees or parties
- Actions taken

Initial Response to Suspicions or Allegations of Fraud

When responding to suspected and detected incidents of fraud, time is critical. Management and fraud examiners must be prepared to address a number of issues in a short amount of time, sometimes under stressful conditions.

This section explores the first steps that management and fraud examiners should take when a fraud-related incident becomes known, and it provides a list of tips for managing and organising the process of responding to suspected and detected incidents of fraud.

Initially, when a suspicion or allegation of fraud arises, management must respond quickly. The failure to act quickly against suspicions of fraud could result in litigation, enhanced penalties, and enforcement actions by government regulators.

The appropriate response varies depending on the facts, such as the underlying evidence, who is implicated, how the evidence came about (e.g., internal sources, civil lawsuit, investigation by the government), and so on. But generally, when evidence of fraud arises, management should respond by engaging in the following actions:

- Activate the response team.
- Engage legal counsel, if necessary.
- Consider contacting the insurance providers.
- Address immediate concerns.
- Conduct an initial assessment.
- Document the initial response.

Activate the Response Team

When evidence of fraud arises, management must activate the fraud response team—the group of people tasked with responding to incidents of fraud. When activated, the response team should seek to answer the following questions:

- Is a formal investigation necessary?
- If a formal investigation is necessary, who will lead it?
- Is there a need for immediate police involvement?
- Is there an immediate need for legal assistance or advice?
- Is there a need for external support (e.g., forensics specialists)?
- Is there a need for additional support (e.g., access to IT facilities or a secure room, support from administration)?
- Is there a need to devise a media strategy to deal with the issue?
- Is there a need to report the issue to an external third party?
- Should the audit committee be informed?

Engage Legal Counsel

Because incidences of fraud are riddled with legal uncertainties, management should consult with internal and possibly external local legal counsel before making any decisions or taking any action concerning the suspected conduct. Typically, the general counsel should be made aware of any significant fraud that might result in legal action.

Consider Contacting the Insurance Provider

When evidence of fraud arises, it is generally impossible to know whether the incident will result in an insurance claim, but even so, many insurance policies require timely notice of potential claims. Therefore, an organisation should consider putting its insurer on notice to preserve a potential insurance claim.

Address Immediate Concerns

Also, when evidence of fraud arises, management and the response team should address immediate concerns. Immediate concerns will vary, but they might include:

- Preserving relevant documents
- Identifying who should be informed

Preserving Relevant Documents

When evidence of fraud arises, management should seek to preserve all relevant documents, especially those that an employee might want to hide or destroy. In a fraud investigation context, the term *documents* typically refers to, but is not limited to, contracts, invoices, correspondence, memoranda, weekly reports, presentations, telephone messages, emails, reports, performance reviews, performance improvement plans, medical records, and other written or recorded material.

When evidence is misplaced, lost, or destroyed, it becomes more difficult to conduct an investigation. Thus, the response team and management must take action to preserve evidence as soon as the decision to investigate is made. There are a number of steps that management should take to preserve relevant documents. For one thing, management should work with legal counsel to issue a litigation hold to notify employees to suspend the destruction of potentially relevant records.

Furthermore, management should suspend the organisation's record retention policy temporarily to avoid a piece of evidence accidentally being destroyed.

Also, management could lockdown access to emails or digital files that employees might want to conceal or destroy. Digital information can be found in virtually any type of media, and it is more fragile than tangible evidence. Therefore, employees can destroy this type of information if it is not protected properly. Often, when fraudsters become aware of an investigation, they try to destroy evidence in their computers or sabotage other evidence that could be used against them. Accordingly, it is a good idea to have IT personnel involved in this process each time the organisation decides to conduct an investigation.

The failure to preserve documents could have several adverse consequences. First, the failure to preserve documents could result in the government's questioning of the integrity of any fraud investigation. Second, documents destroyed when litigation is expected, or in progress, might give rise to claims of spoliation of evidence, which, if proven, could lead to monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defences. *Spoliation* is broadly defined as the act of intentionally or negligently destroying documents relevant to litigation.

In today's digital environment, digital spoliation is a major concern for organisations involved in litigation. When compared to the spoliation of tangible documents, digital spoliation carries additional risks. Management often lacks sufficient knowledge of the inventory of digital information, and electronic data might only be available for an evanescent time. Additional concerns include business practices designed to free up storage space by deleting digital information and the fact that electronic data can reside in numerous locations, as well as the fact that identifying relevant electronic data within today's large and complex data systems can be challenging and costly.

Identifying Who Should Be Informed

Management and the response team should identify whom to inform. Depending on the facts, several departments should be interested in fraud, including legal, human resources, internal audit, security, risk management, and loss prevention or security. When responding to an allegation of fraud, it is important to consider the interests of each of these departments. This is necessary to ensure that designated employees are notified immediately to enable a prompt response. Information about incidences, however, should be shared only on a need-to-know basis.

Human resources (HR) personnel address issues involving unfair treatment, discrimination, harassment, substance abuse, or concerns about corporate policies. Therefore, the HR department should be informed of fraud that affects any such areas.

Both the HR and legal departments should be involved to ensure that the right people receive information in a timely manner. Also, other departments, such as loss prevention and risk management, audit, and security might need to be involved. Although the development of information distribution rules requires the participation of several departments, it is best to have these rules set before investigation protocols are in place.

Another department that needs to be involved is the information technology (IT) department. The IT department might need to be part of an investigation to safeguard data until it can be analysed. IT personnel can also help identify what data are available and where, and they might be able to function as forensic investigators if licensed to do so.

Again, management must restrict access to certain pieces of information on a need-to-know basis.

Conduct an Initial Assessment to Determine the Appropriate Response

Usually, when an allegation of fraud arises, there are not enough known and verified facts to begin a formal investigation; therefore, management and the response team should conduct an initial assessment to determine if an investigation is needed and what steps, if any, are required to respond in an appropriate manner. This is perhaps the most critical question that management must answer when an allegation of fraud arises.

An initial assessment should be quick and, unless complications arise, completed within a few days. Ideally, action should be taken within three days of learning about an incident.

The initial assessment should be a limited fact-finding analysis focused on the specific allegation or incident. It does not require an investigation plan or report, unlike a formal investigation. Thus, the initial assessment should seek to:

- Determine if fraud occurred.
- Identify the status of the fraud (e.g., When did it begin? Was it internal or external? Is it still occurring? If it is no longer occurring, when did it stop?).
- Identify potential claims and offences.

To conduct an initial assessment and determine the appropriate response, those responsible should take the following steps:

- Understand the context.
- Review any applicable policies and procedures.
- Investigate the allegations.
- Document the reasons for the decision.

Understand the Context

Next, those responsible should gain an understanding of all of the circumstances leading up to the current situation. Often, the context is necessary to determine the best approach to dealing with a tip or suspicion, and it can provide clues that are helpful in other areas. Efforts to understand the context should seek to obtain the initial facts and circumstances about:

- The manner in which the suspicions became known
- The date suspicions became known
- The areas to which the suspicions pertain
- The source of the information
- The allegations at issue

Review Any Applicable Policies and Procedures

Those involved in the initial assessment must also review any applicable internal controls and organisational policies, including any anti-fraud auditing and testing policies and procedures, to determine the best method and processes for continuing the investigation.

Investigate the Allegations

An initial assessment should be a limited, fact-finding analysis, and it should focus on investigating the specific allegation or incident. More specifically, to determine the appropriate response, the assessment should, if possible, seek to answer a number of questions, including:

- Is the allegation credible?
- Who is the subject of the allegation, and what is his relationship to the company?
- When did the alleged misconduct occur, and how often did it occur?
- What was the business purpose of the activity related to the allegation?
- How serious is the allegation?
- What levels of employees are alleged to be involved, if any, in the misconduct (i.e., officers, directors, or managers)?

- What individuals might have pertinent information about the matter that would tend to support or refute the complainant's position, and what facts do these individuals purportedly know?
- Did any third parties receive any direct or indirect benefit from the misconduct, and if so, who are they?
- If a third party is involved, is the third party a government official?
- How was the matter recorded on the company's books and records, if applicable?
- Can it be determined if the person in question acted with fraudulent intent?
- Is it possible that the issue might be larger than expected?
- Were there any whistleblowers, and if so, how should they be dealt with?
- What measures should the company take to document how the initial evidence of wrongdoing was handled?
- Is the government already involved, and if not, is it likely that the government will become involved?
- Is it likely that the matter will have significant negative impact on shareholder value?

These questions are important because the response should be proportional to the potential scale of the fraud in terms of its value, frequency, potential damage, the individuals involved, the number of people involved, and so on.

In addition, the decision as to the appropriate response might be influenced by other factors. As with any business decision, the cost of conducting the investigation must be considered, and management might also consider whether an investigation will interrupt business activity.

Generally, the investigation portion of the initial assessment will involve:

- Contacting the source, if the investigation was triggered by a report or complaint
- Interviewing key individuals
- Reviewing key evidence

CONTACTING THE SOURCE

If the evidence came in through a tip from an identified source, those responsible should contact the source to find out additional information and confirm the source's willingness to help throughout the investigation. When contacting the source, the interviewer should

encourage the complainant to provide a narrative description of the report. After the source provides the narrative, the interviewer should ask clarifying questions and then summarise the key points.

An interview with the source should seek to determine:

- What does the individual know?
- How did the individual get the information?
- Who were the key individuals involved?
- When did the alleged events occur (e.g., dates, times, and locations)?
- What are the details (e.g., who, what, when, where, why, and how much) of the allegations?
- What are the dates (or period) of the key events?
- What evidence exists to corroborate the alleged events, where is the evidence located, and how can the evidence be accessed?
- What witnesses can corroborate the alleged events?
- Which individuals might have pertinent information about the matter that would tend to support or refute the complainant's position, and what facts do these individuals purportedly know?
- What was the motivation behind the alleged events?
- Why were the alleged actions improper?
- If the scheme is ongoing, do the subjects know of the complainant's report?
- What is the complainant's motivation for making the report (e.g., What prompted you to report this?)?

When interviewing the source, the interviewer should seek to determine if there is any reason to suspect the complainant's credibility. Also, if there are any weaknesses in the complainant's information, the interviewer should ask the complainant to explain what he expects the subject would say in defence of the allegations and ask the complainant to explain why such a response is not sufficient to dispose of the matter. Additionally, the interviewer should ask the source what he wants the organisation to do about the complaint. The response to such an inquiry will help the team focus its efforts.

INTERVIEWING KEY INDIVIDUALS

Those responsible should interview key individuals for information about the suspicious conduct and the subject(s). Interviewing individuals with personal knowledge is critical.

Also, they should interview witnesses as early as possible because it will limit the harm arising from loss of memory, witnesses becoming unavailable, and inadvertent loss or destruction of key evidence.

REVIEWING THE EVIDENCE

Those responsible should review relevant documents and files, which might include personnel files, the organisation's employee handbook, accounting records, vendor activity reports, budget reports, fixed asset records, expense reimbursements records, leasing documents, rental agreements, payroll records, purchasing requisitions, purchase contracts, inventory records, shipping/receiving reports, emails, telephone records, and so on.

Obtaining and reviewing these documents will assist in understanding the chronology of events and might put the responsible parties on notice as to certain strengths or weaknesses of the investigation.

Document the Reasons for the Decision

To avoid any real or perceived downplay of the matter's significance and to avoid any attempts at wilful blindness, those responsible should document their actions and findings. In addition, management must document its decisions and the reasons behind them. Thus, if management decides against conducting an investigation, it must document the reasons why.

Again, management should document the organisation's initial response in an incident report log that serves as a record of the organisation's response efforts. Once a suspicion of fraud arises, the issue should be recorded and detailed in the log. As the issue progresses, the log should be modified and, ultimately, it should contain details of actions taken and conclusions reached.

The incident report log should contain all information relevant to or created during the initial response that is used to support management's decision making.

Planning and Conducting a Formal Investigation

Once it is determined that an allegation or issue will be investigated, those responsible must begin the formal investigation. Typically, the steps involved in this process include:

- Completing engagement letters/contracts, if applicable
- Assembling the fraud team

- Learning about the organisation at issue
- Developing an investigation plan

Completing Engagement Letters/Contracts

Certified Fraud Examiners are sometimes hired for specific engagements, and in such cases, it might be preferable to document the engagement in a formal written contract or a client engagement letter. (In some circumstances, an oral understanding might be sufficient.)

Engagement contracts or retainer agreements are beneficial for various reasons. For one thing, they will maximise a fraud examiner's protection in the event of a client dispute or misunderstanding, making later disputes about the engagement's terms easier to resolve. For another thing, engagement contracts or retainer agreements will help manage client expectations by making the assignment's objectives clear.

It is important to note, however, that although formal, written agreements might be preferable, they are not always practical.

Engagement letters should be written with certain standards in mind, and they should address a variety of items. Those items include, but are not limited to, the client's identity, the scope of the services, the timing of the work, deliverables, payment terms and fee structure, communication with the client, non-guarantee, governing law, jurisdiction, termination, and limitation of liability through indemnity clause.

There are two primary forms of engagement letters: the long form and the short form. The *long form* spells out the details of what examination techniques the fraud examiner intends to follow, while the *short form* does not. See the Sample Fraud Examination Reports in Appendix E (located at the end of the Investigation section of the *Fraud Examiners Manual)* for examples of each type of engagement contract.

Although engagement letters contain various items, they contain the following basic parts:

- Opening
- Body (long or short)
- Terms
- Indemnity clause
- Close

Opening

The opening paragraph should state the purpose of the engagement. It should be specific as to whether the letter is an engagement or a proposal letter.

Body

The body of the letter will follow either the long form or the short form.

THE LONG FORM

The long form is similar to an engagement letter prepared for specific-scope examinations performed by auditors. In the body of the long form, the fraud examiner describes the procedures in detail and limits the scope of an examination to the procedures defined. This form is not recommended for engagements that require the investigation of fraud allegations and a concluding opinion on the existence of fraud.

At the onset, the fraud examiner might not know what procedures will be necessary to resolve the allegation, and in such circumstances, it will be difficult to describe the anticipated procedures with any precision.

THE SHORT FORM

The short-form engagement letter outlines the general scope of the engagement. For example, it might describe that the services will include an investigation of a fraud allegation received over the hotline, by an anonymous tip, or by an audit anomaly.

The short form might also confirm whether the fraud examiner has access to any personnel or documentation deemed necessary to carry out the assignment. This type of engagement letter is best used for work that will ultimately require an opinion on a fraud allegation. Because the fraud examiner will not know the nature of the alleged fraud at the onset, it is best to avoid limiting the examination's scope.

Terms

The terms paragraph of an engagement letter should include the payment terms, fee structure, and the method of payment. The terms should include a retainer, if needed, and it should indicate how many hours of examination time the client initially agreed upon. Additionally, this section should describe the billing procedures and a statement regarding payment methods.

Also, the terms should address out-of-pocket expenses. If travel is required, for example, the terms should discuss the anticipated cost of travel and the number of trips.

This section should include things such as:

- The fraud examiner(s) assigned to the case
- The fraud examiner's hourly rate, if he bills at a flat rate
- If there is a retainer, the terms section should include a statement regarding the exhaustion of the retainer, what expenses will be reimbursed if there are unused retainer proceeds, and when and how such reimbursements will be refunded
- A policy regarding past due invoices and late fees, including finance charges if applicable
- Rates for any additional services or expenses that might be needed

Indemnity Clause

In letters of engagement, there should be an indemnity clause to protect the fraud examiner if the subject, a witness, or a third party sues the client and includes the fraud examiner as a party to the suit. The clause should not be boilerplate; it should be tailored to fit the particular terms of the engagement.

The indemnity must be broad enough to cover the fraud examiner's legal expenses, provide for independent counsel, and protect the fraud examiner from liability in case of an adverse finding, but it should also provide for the cost of time and expenses of the fraud examiner at the fraud examiner's usual hourly rate.

It can be extremely frustrating and expensive to spend days in court working on someone else's case with no retainer.

SAMPLE INDEMNITY CLAUSE

[Client company] agrees to indemnify and hold harmless [fraud examiner's company], its personnel, agents, subcontractors, and consultants from and against any and all claims, liabilities, cost, and expenses, including labour arbitration or related proceedings, (including without limitation, independent legal representation of [fraud examiner company]'s choice, attorney's fees, and the time of [fraud examiner's company] personnel, operatives, and consultants involved to defend or appear at any judicial or quasi-judicial proceedings), brought against, paid, or incurred by [fraud examiner's company] as a result of any of its services provided to [client company] in this project.

This includes, but is not limited to, any claims arising from violations of any laws relating to personal injury or property damage whatsoever suffered by [client company], its employees, or third parties. This provision shall survive the termination of this agreement.

Close

The closing section should conclude the letter. It should thank the addressee for the opportunity, and it should include the fraud examiner's contact information where he can be reached.

Also, the closing should include the date of agreement, client signature, printed name, client's contact information, and the fraud examiner's signature. The fraud examiner should ask the addressee to sign one copy and return it in a self-addressed stamped envelope.

Assembling the Fraud Team

Fraud examinations usually require a cooperative effort among different disciplines; therefore, if members of management decide to investigate suspicions of fraud, they must determine who should lead and be involved in the investigation.

To determine this, management must identify the needed skills. Typically, fraud investigations require skills across different disciplines and industry sectors. Auditors, fraud examiners, managers, attorneys, security personnel, and others are frequently associated with fraud investigations.

Selecting the right team members is essential for an effective fraud examination. Accordingly, when choosing the participants in an investigation team, it is critical to identify those who can legitimately assist in the investigation and who have a legitimate interest in its outcome. These persons should be included on the investigation team, and all other personnel should be excluded from the team.

Also, when organising the team, it is important to consider all of the implications that might arise from an investigation. These implications include the business, legal, human resources, and operational factors that arise when an investigation commences. Addressing these potential issues up front will ensure that significant factors (e.g., the team members' abilities, the leading executives, and the assurance of independent action and reporting) are considered.

Furthermore, the team should comprise professionals with the skills needed to deal with various types of incidents. To acquire the appropriate level and mix of skills, the team should include internal resources (if available) and external resources, if needed or appropriate.

Typically, team members should have:

- Accounting and audit knowledge
- Knowledge of the industry
- Knowledge of the organisation
- Knowledge of the law and the rules of evidence in the jurisdiction where the fraud occurred
- Knowledge about privacy issues in the jurisdiction where the fraud occurred and where the investigation will occur
- An understanding of psychology and motivational factors
- Interviewing skills, in the native language
- Communication skills
- Computer skills

A successful fraud examination, however, depends not only on the knowledge and skills of individual members, but also on the individual team members' characteristics that facilitate team interaction and functioning. These characteristics are especially critical for teams that require more coordination.

After identifying the necessary skills and characteristics, management must determine who possesses them and begin selecting the team. Each team will vary, depending on the goals, circumstances, and people involved.

Common Types of Professionals

A typical fraud examination team might include the following types of professionals:

- Certified Fraud Examiners (CFEs)
- Legal counsel
- Local international counsel
- Accountants or auditors (internal or external)
- Forensic accounting investigators
- Forensic technology experts
- Audit committee members
- Security personnel

- Human resources (HR) personnel
- A management representative
- Information technology (IT) personnel
- Computer forensic experts
- Data analytics specialists
- External consultants
- Industry specialists

CERTIFIED FRAUD EXAMINERS

Certified Fraud Examiners (CFEs) are trained to conduct complex fraud cases from inception to conclusion. A CFE has training in all aspects of a fraud examination and can therefore serve as a valuable "hinge" to the investigation team, tying together the financial examination and the more traditional investigative techniques.

LEGAL COUNSEL

It is crucial to have legal counsel involved in, and in most cases, "directing," fraud examinations, at least as far as the legal aspects of the process are concerned (e.g., reporting results, preserving confidentiality, avoiding lawsuits, or terminating employees for wrongful misconduct). This is because fraud examination can be a veritable hornet's nest of legal questions, and the team must have legal counsel on hand to sort out these questions. Otherwise, the investigating organisation risks exposing itself to greater danger than the threat it is investigating.

In addition, by having an attorney directing the investigation, or overseeing an investigation conducted at the attorney's request, the company might be able to protect the confidentiality of its investigation under certain legal privileges and similar forms of protection.

LOCAL INTERNATIONAL COUNSEL

Management should obtain the help of local international counsel before beginning a fraud investigation involving work abroad.

Local international counsel is needed to address a number of issues that arise when working in foreign jurisdictions. For example, local counsel will be able to provide advice concerning applicable privileges. Likewise, consulting with local counsel can provide guidance as to whether local laws afford employees privacy rights that might interfere with the investigation.

ACCOUNTANTS OR AUDITORS (INTERNAL OR EXTERNAL)

Because accounting and audit knowledge is necessary to most fraud examinations, a team might include accountants or auditors, whether internal or external. Auditors can support the investigation with information on company procedures and controls. Internal auditors are often used to review internal documentary evidence, evaluate tips or complaints, schedule losses, and provide assistance in technical areas of the company's operations. Additionally, auditors can assess the probable level of complicity within the organisation, and they can help design procedural methods to identify the perpetrators and help determine the extent of the fraud.

FORENSIC ACCOUNTING INVESTIGATORS

A forensic accountant can provide various services, including audits; accountant performance reviews; and examinations of financial documents for fraud, misconduct, or industry standard violations. Moreover, these experts can mine and analyse large amounts of data to identify potentially irregular transactions and high-risk relationships.

AUDIT COMMITTEE MEMBERS

As a result of the passage of the Sarbanes-Oxley Act and similar legislation in many other countries, audit committees are taking a more active role in internal investigations. This has occurred, in part, because such legislation mandates that audit committees for publicly traded companies be directly responsible for two key components of an effective fraud prevention programme—outside audits and internal reporting mechanisms. Accordingly, a company's audit committee might actively oversee a fraud examination or require that the investigation team report directly to it.

SECURITY PERSONNEL

Security department investigators are often assigned the investigation's fieldwork responsibilities, including interviewing outside witnesses and obtaining public records and other documents from third parties.

HUMAN RESOURCES PERSONNEL

The human resources (HR) department should be consulted to ensure that the laws governing the rights of employees in the workplace are not violated. Such involvement will lessen the possibility of a wrongful discharge suit or other civil action by employees. Also, involving HR personnel can help provide access to the organisation's policies and any

employee information that might be needed. Moreover, HR can help the team understand office procedures, and if needed, it can help place suspect employees on paid leave if necessary.

Although the team might need advice from a human resources specialist, normally this person would not directly participate in the investigation.

MANAGEMENT REPRESENTATIVE

A representative of management or, in significant cases, the audit committee of the board of directors should be kept informed of the progress of the investigation and should be available to lend necessary assistance.

INFORMATION TECHNOLOGY PERSONNEL

If fraud occurs, it is likely that a computer was involved. If so, information technology (IT) department personnel might need to be part of an investigation to help identify what data is available and where it is located, as well as to help safeguard the data until it can be analysed.

COMPUTER FORENSIC EXPERTS

When developing a fraud examination plan, management should determine whether a computer forensic expert is needed.

In today's world of increasing technologies, more and more information is created, stored, and disseminated electronically. Due to the sensitivity of digital evidence, the team should include a computer forensic expert if an investigation involves more than cursory analysis of electronic evidence. Moreover, with the majority of communication being conducted electronically, emails can be used as evidence in just about any case.

Computer forensic experts can uncover a large amount of data that relates to the use of a computer, what is or has been stored on it, and the details about the computer's users. Additionally, computer forensic experts might be able to recover evidence that a non-expert cannot. For example, if the target of an investigation tries to delete electronic evidence, a forensic expert might, depending on when and how the files were deleted, be able to recover the deleted files. Similarly, a forensic expert might be able to get around encrypted information.

Also, it is important to allow a trained examiner to conduct a proper seizure and examination of digital evidence to help ensure that the information can be used in a legal proceeding. Within the computer forensics field, there are several different types of special experts. Given the diversity of computer-related fraud, no person can be an expert in all aspects of computer technology.

Moreover, in cases involving litigation, a forensic expert can help parties draft interrogatories and requests for production designed to solicit relevant data, and they can help prepare and participate in depositions involving record custodians.

DATA ANALYTICS SPECIALISTS

As the volume of electronic records continues to grow, it is increasingly necessary for investigation teams to include data analytics specialists. These specialists are adept at searching, collecting, extracting, cleansing, analysing, and modelling data. Thus, data analytics specialists can help manage costs, especially in larger, more complex investigations.

EXTERNAL CONSULTANTS

When conducting a fraud examination, fraud examiners should determine whether a technical specialist is needed for assistance.

Additionally, when the suspect employee is particularly powerful or popular, it might be useful to employ outside specialists who are relatively immune from company politics or threats of reprisals.

INDUSTRY SPECIALISTS

In some cases, it might be necessary to include an individual with deep industry knowledge. Industry specialists can help develop the investigation plan, evaluate technical documents, and identify potential misstatements by interviewees.

Dos and Don'ts for Selecting Team Members

The dos for selecting team members include:

- Consider the team's size.
- Check for conflicts of interest between internal and external team members.
- Ensure that there are no reporting issues (e.g., a team member feels pressure to report all details of the investigation to his direct manager, even though his manager does not have

a need to know). Reporting issues can be prevented by establishing confidentiality rules in the beginning of the investigation.
- Select team members that fit the investigation's demands and objectives.
- Recruit team members with the skills needed to conduct the investigation.
- Recognise the unique knowledge, experience, and skills that each team member can contribute.
- Contemplate the ways that each potential member will fit into the team.
- Select people who will work well with other team members.

The don'ts for selecting team members include:
- Don't select team members based on friendship.
- Don't select team members to repay a favour.
- Don't select team members with negative attitudes.
- Don't overlook team members with untraditional knowledge that can contribute to the investigation (e.g., people with experience in a particular industry).
- Don't select members who might have personality conflicts with other members.
- Don't select members with a vested personal or corporate interest in the matter.
- Don't select members with a close personal or professional relationship with the subject or the complainant.
- Don't select members who lack restraint and a sense of discretion.

Identify the Investigation Leader

When evidence of fraud arises, management must designate someone to lead the investigation. A leader should have investigative experience and knowledge of legal and compliance requirements regarding the specific issues involved.

The investigation leader should be determined based upon the seriousness of the allegation. Management should consider whether to appoint an internal party (if available) or an external third party to lead and oversee the investigation.

The leader should be independent of the activity affected by the alleged fraud and have the means to recruit resources necessary to conduct the investigation, sufficient authority and access to gather any necessary information, and the ability to communicate with senior management.

Learning About the Organisation at Issue

When tasked with conducting a fraud examination involving an organisation, the team must become familiar with (if it isn't already) the organisation, its industry, its competition, its market share, its financing structure, its vendors (suppliers), its customers, its methods of receipts (i.e., case or on account) and disbursements, its procurement methods, its economic climate, its recordkeeping system, its policies and procedures, its organisation chart and job responsibilities of key employees, and other matters that might be relevant to a fraud examination.

Understanding the entity will enable the team to assess the risks associated with the entity's particular operations.

Developing an Investigation Plan

Once it is determined that an allegation or issue will be investigated, those responsible should develop an investigation plan.

Each member of the team should be involved in the planning process. Letting each team member contribute to the planning process increases the likelihood that everyone will buy into the plan and results in a team approach that draws on each member's expertise.

The team should start planning early and update the plan throughout the investigation. Planning is not a one-time event; it is an ongoing process that requires constant attention, and the team must refine their plan as the facts and client's (or employer's) needs change.

Each fraud investigation is different, and no single plan can cover every situation. The facts and circumstances of each case should shape how an investigation is structured, what procedures are performed, and how those procedures are carried out. Nevertheless, it can help to have a standard set of items from which to begin the planning process.

In short, when developing an investigation plan, those responsible should:

- Review what is known and gain a basic understanding of key issues.
- Define the goals of the investigation.
- Identify whom to keep informed.
- Determine the scope of the investigation.
- Establish the investigation's timeframe.
- Address the need for law enforcement assistance.

- Define members' roles and assign tasks.
- Address operational issues.
- Outline the course of action.
- Adapt the necessary resources to conduct an investigation.
- Prepare the organisation for the investigation.

Review What Is Known and Gain a Basic Understanding of Key Issues

The known information should serve as the basis for the plan. So, before writing the investigation plan, the fraud examiner must review what is known and gain a basic understanding of issues that are key to planning the investigation.

Typical questions to answer before beginning a fraud examination include:

- What period is under review?
- What is the timeframe?
- What are the deadlines?
- What is the nature of the suspected fraud?
- Where are the relevant locations?
- Who is the contact at the locations?
- Who are the targets?
- Does the issue predate any of the key players?
- Have any related fraud examinations ever been conducted at the relevant location?
- What other entities, departments, or regions might be involved?
- How long has the issue existed?
- What is the culture of the industry or department at issue?
- What other sites might be involved?
- Does the organisation perform background checks of employees as a precondition of employment?
- Did the suspected fraud occur in an industry or location that has a history or culture of fraud?
- Has the organisation been in compliance with reporting and regulatory requirements?
- What is the profitability of the unit or organisation at issue in the investigation?
- Does the organisation's level of growth make sense in light of its industry and peers?
- Has there been a recent acquisition, and if so, is former management still in place?
- Does the organisation have a fraud policy?
- What type of report (written or oral) does the client expect?
- What is the budget?

After the fraud examiner obtains a basic understanding of the key issues, he can begin developing the investigation plan.

Define the Goals of the Investigation

An investigation must have goals or a purpose, which should be identified at the outset so the team members can achieve them. Goals also help keep the investigation focused and on task, and they can serve as an energizer, as long as they are specific, well defined, and measurable. A specific goal is more likely to be achieved than a general goal. If goals are not well defined, the team cannot expect to reach them, and goals must be realistic within the availability of resources, knowledge, and time. Measurable goals will allow the team to determine attainability, estimate a timeline, and know when the goals have been achieved.

Although the basic goal for most fraud investigations is to determine whether fraud occurred, and if so, who perpetrated it, fraud investigations might be designed to achieve a number of different goals, such as to:

- Prevent further loss or exposure to risk.
- Determine if there is any ongoing conduct of concern.
- Establish and secure evidence necessary for criminal or disciplinary action.
- Minimise and recover losses.
- Review the reasons for the incident, investigate the measures taken to prevent a recurrence, and determine any action needed to strengthen future responses to fraud.
- Help promote an anti-fraud culture by making it clear to employees and others that management pursues all cases vigorously and takes appropriate legal or disciplinary action where it is justified.
- Protect the company's legal privileges.

Identify Whom to Keep Informed

At the outset of a fraud examination, the investigation team and management must identify whom should be kept informed about the investigation. In general, as few people as necessary should be kept informed.

Factors to consider when determining whom should be kept informed include the severity of the incident under investigation, the suspect's role in the organisation, and the tasks that will be required to conduct the investigation.

Determine the Scope of the Investigation

When planning an investigation, the stakeholders should identify the *scope* (the boundaries or extent of the investigation), which will vary depending on the facts and circumstances. An investigation, for example, might be limited to the subject matter, the department, or the geographic area at issue.

To determine the scope, those responsible should use the following guidelines:

- Consider the ultimate goals of the investigation.
- Develop a list of key issues raised in the initial assessment.
- Determine the level of discretion that is required.
- Determine if there are any constraints (e.g., time, resource, authority, procedural, legal, or practical). (Identifying such limitations helps ensur that the team can meet realistic objectives and develop alternative strategies.)
- Consider the quality of the organisation's anti-fraud programme and policies.
- Consider the organisation's actual culture of compliance.
- Determine the extent to which mid- and senior-level management is involved in the suspected misconduct.
- Determine whether the issue is widespread or isolated to a particular area.
- Ascertain whether the suspected misconduct was prohibited by the organisation's compliance programme.
- Consider broadening the scope if the allegations indicate a failure in the organisation's compliance programme.
- Consider what the government expects.

Additionally, to determine the scope, the team and management should also consider how the issue became known (i.e., what prompted the investigation). Fraud issues can stem from a number of different sources, and different sources prompt different responses. If, for example, the issue arose out of a government investigation, the company's investigation should shadow the government's actions.

Establish the Investigation's Timeframe

When planning the investigation, the team must establish proper time parameters with start dates and due dates for tasks and deliverables. Also, the team should obtain the dates of upcoming earnings releases and audit committee meetings.

An established timeframe helps the team provide a quick and appropriate response, which can help the subject organisation avoid future legal disputes and minimise adverse impact on employee morale.

In addition, time parameters will help the team members structure their plans, providing information to help develop concrete, short-range actions to reach the investigation's goals.

Address the Need for Law Enforcement Assistance

The planning stage of the investigation should also include efforts to consider the need for law enforcement assistance. That is, management must decide if the matter at issue is serious enough to call in the police or other law enforcement entities. Whether to seek assistance from law enforcement can be a difficult decision for organisations to make.

If, at the beginning of the investigation, management determines that it will make a formal referral to law enforcement or a prosecuting agency, then it must notify the authorities before the investigation commences to determine whether law enforcement personnel should participate in the examination.

Define Members' Roles and Assign Tasks

The team's authority levels, responsibilities for action, and reporting lines should be defined during the planning process. For efficient and effective coordination, all team members must be clear about their roles and responsibilities and the investigation's goals. Also, defining the members' roles and responsibilities gives them purpose and checkpoints for measuring success.

Conversely, failure to define roles and responsibilities can have an adverse impact on an investigation. Without clear roles, the team might waste time and money, gaps in the investigation process might appear, or the investigation might lead to incomplete or faulty results.

That said, delineating the team members' roles is difficult because fraud investigations often are conducted in an unstable and high-pressure atmosphere that disrupts communication. Nevertheless, it needs to be a priority for management and individuals on the team.

In general, team members should understand:

- Their expected roles and responsibilities
- The expected roles and responsibilities of other team members
- The degree and source of any outside scrutiny
- Timing issues
- Expected form and timing of interim deliverables or final product
- Expected timing of interim deliverables or final product
- Specific facts of the matter at issue
- Limitations on who can be involved in the investigation

Moreover, if the organisation at the centre of the investigation does not have a pre-established line of authority in its fraud policy or investigative protocols, the investigation plan should define the team's authority levels, responsibilities for action, and reporting lines. This allows for efficient and effective coordination.

Management should designate a primary contact person with whom the team can communicate on all matters that arise during the investigation. It is essential that the team reports to someone who will take action pursuant to the investigation's findings.

Address Operational Issues

During the planning process, management must consider any operational issues, which might include:

- Gathering facts abroad
- Recordkeeping practices abroad
- Record content and format differences
- Language translation
- Cultural differences
- International data privacy issues
- Differing conceptions of privacy and discovery
- Immigration regulations
- Safety concerns, especially for global assignments

Among the issues listed, international data privacy laws are of particular concern. Many foreign countries—and those in the European Union (EU) in particular—restrict or prohibit processing and transferring personal data. For example, the EU's directive on personal data protection (EU Directive), which has served as a model for the personal data protection laws

of Argentina and Poland, essentially requires consent to use personal data and places limits on transmitting personal data to non-EU countries. Thus, the data privacy laws of other countries can significantly affect data collection, data use, and cross-border transfer.

Similarly, recordkeeping practices in other countries differ, and this could cause difficulties when attempting to obtain information in foreign countries.

Outline the Course of Action (Create a Roadmap/Case Plan)

Before beginning a fraud examination, the investigation team should develop a case plan to make sure it addresses every relevant issue. A case plan outlines the course of action the team members expect to take throughout the investigation, and establishing a case plan helps the team stay on track and focus on the key issues.

The case plan can encompass matters such as:

- The scope of the investigation
- The goals of the investigation
- Time parameters
- Resources needed
- Task assignments
- The overall approach to conducting the investigation

Also, the case plan should, among other things, outline how and in what order the team will proceed. Those responsible should organise an investigation by breaking it down into smaller, more manageable components. It is important, however, to avoid excessively breaking down an investigation, because doing so can lead to micromanagement or inefficient work management.

There are many ways to organise an investigation's components, but often, investigations are organised in the following ways:

- *Chronologically:* A chronological investigation is divided into time-based phases that, when completed, are marked as milestones. The phases are the broad steps needed to complete the investigation, and each phase contains tasks that define the actions needed to reach each milestone. The tasks should be assigned based on who is best suited to perform them. Milestones indicate the investigation's overall progress. This structure is best suited for investigations where time sequence is essential in organising tasks.

- *By functional area:* This approach organises investigations by functional areas needed to accomplish the investigation's goals. Thus, this approach focuses on the type of activities and processes that must be done under each functional area.
- *By team member:* This method of organisation involves organising the investigation's work by each member's area of expertise.
- *Hierarchically:* This approach organises the members' roles and tasks hierarchically, from major undertakings to minor undertakings. Thus, the components are organised based on their relationship to each other.

Also, because the case plan should outline how and in what order the team will proceed, it should identify the information that is necessary to complete the investigation and include the investigative activities to be performed, such as:

- Documents and evidence that should be located, obtained, and examined
- A list of witnesses and subjects to interview and the preferred order of the interviews
- The date that a report of the investigation should be presented
- Matters that need supervisory review and approval

When developing the case plan, the team should consider:

- How to most efficiently achieve the goals of the investigation
- How to accomplish the goals of the investigation on a timely basis, with appropriate confidentiality and fairness to all parties
- How to ensure that the investigation's results are thorough, accurate, and documented appropriately
- How to ensure compliance with the law and the organisation's policies and procedures

Moreover, the circumstances will change and new information will emerge during the course of an investigation, so the team and the plan must be adaptable.

Each stage of the investigation should be documented. Documenting the planning process will demonstrate advance thought and preparation, and will show thoroughness and help counter challenges that the investigation was inadequate.

It is helpful to prepare to-do lists or checklists for an investigation. For reference, a sample checklist is located in Appendix B. The sample checklist, however, is not intended to cover all aspects of the examination, but rather to provide the examination team with planning assistance.

Adapt the Necessary Resources

As with any special investigation or operation that requires advance preparation, the planning process in a fraud investigation must include efforts to adapt the resources needed to deal with the variety of issues that might occur during the course of the investigation. A successful fraud investigation requires support from management, the right supplies, adequate funding, and any other identified resources.

That is, the investigation team needs to have the tools necessary to complete the investigation. This is especially true if the relevant operations are in developing economies, remote locations, or areas with a higher risk of security-related incidents.

The necessary resources might include:

- Outside specialists
- Case management software
- Digital forensics tools (e.g., EnCase or Forensics Toolkit)
- Access to a commercial database

Also, every team member should have the contact information for those involved in the investigation.

Prepare the Organisation for the Investigation

Before commencing a formal investigation (and especially before starting the evidence collection process), it might be necessary to prepare the subject organisation for the investigation. Preparing an organisation for an investigation involves such things as:

- Prepare the managers of the employees who will be involved in the investigation, especially if they do not know about the issue. Let them know that the subject and witnesses might be busy at times during the investigation. The amount of information to share with a manager will depend on the circumstances.
- Notify key decision makers when the investigation is about to begin.
- Notify the organisation's in-house or outside counsel when the investigation is about to begin.

But generally, it is not good practice to alert all of an organisation's employees that an investigation will be taking place, nor should the investigation's purpose be explained to all employees.

Structure the Investigation to Preserve Confidentiality

Fraud investigations must be structured to preserve confidentiality. If confidentiality issues are not given attention from the outset of the investigation, the details of the investigation might become public, compromising the entire investigation. Additionally, if the details of the investigation do not remain confidential, employees will be reluctant to report future incidents, and if the suspicions giving rise to the investigation prove unsupported, the reputations of those suspected of misconduct might be irreparably damaged. Moreover, if an investigation stems from a complaint and the complaint becomes known, it is possible that the complainant could be retaliated against.

Accordingly, those responsible must structure the investigation to preserve confidentiality. Among other things, the team members should:

- Avoid tipping off the suspected fraudster(s).
- Request participants' confidentiality.
- Guard case information.
- Consider conducting the investigation under any applicable legal privileges.

Avoid Tipping Off the Suspected Fraudster(s)

When responding to a sign or allegation of fraud, those responsible must work to avoid tipping off those suspected of fraud.

If the suspect is tipped off, a number of different adverse events might occur. For instance, the fraudster might attempt to destroy or alter evidence, making it more difficult to conduct the investigation. When investigation details are leaked, concealment and destruction of evidence typically occurs at a faster rate.

Additionally, a tipped off suspect might attempt to flee, cut off contact with associates, or try to place the blame on somebody else.

Because tipping off the fraudster is a key concern in any investigation, the confidentiality of an internal investigation is critical. To avoid tipping off those suspected of misconduct, it is important to have information about the person who is being investigated and what he can access. Also, to maintain confidentiality, determine in advance who should receive information about the investigation and reevaluate who should receive information as the investigation proceeds.

Here are some basic measures organisations and fraud examiners can take to avoid tipping off suspected perpetrators who are under investigation:

- Know who is being investigated and what they can access.
- Limit the extent of any discussions.
- Only inform those who need to know.
- Inform employees of the consequences of a confidentiality breach.
- Work discreetly without disrupting the office's normal course of business so that employees do not know that an investigation is being performed.
- Work fast.
- Investigate during off hours.

Moreover, it is important for fraud examiners to be knowledgeable about the subject organisation's guidelines or policies. Do the applicable guidelines or policies have a need-to-know clause and an all-access clause? Such clauses will allow the team to keep the details of the investigation confidential, and will provide the investigator with access to all the company systems so he can gather as much system evidence as possible without notifying any internal parties.

Finally, if the suspect is tipped off, management should adjust the investigation and its timeline accordingly. This might mean interviewing the fraudster out of sequence from a normal investigation.

Request Participants' Confidentiality

To preserve the confidentiality of an investigation, management might (if legally permissible) remind participants to refrain from discussing investigation information with anyone or require participants to sign a confidentiality oath vowing not to divulge any information regarding the investigation.

Generally, an employer can ask employees to keep an investigation confidential when there are legitimate business justifications for making such requests.

But typically, management should not implement a blanket policy prohibiting employees from discussing employee investigations because doing so could violate certain rights of the employees. Some jurisdictions guarantee private-sector employees the right to organise and engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection. And if an employer that operates in a jurisdiction that affords employees

such rights has a routine policy or practice of asking employees not to discuss matters that are under investigation, the policy or practice might violate the employees' right to organise and engage in other concerted activities.

Guard Case Information

To help preserve confidentiality, the investigation team members should guard case information. Here are some recommended procedures for protecting case information:

- Store all confidential documents in locked file cabinets or rooms accessible only to those who have a business need-to-know.
- Protect all electronic information via firewalls, encryption, and passwords.
- Clear desks of any case information before stepping away.
- Lock computers when leaving workstations.
- Mark all case information, whether tangible or electronic, as confidential.
- Avoid talking about the investigation in public or in any place where other employees could hear the communications.
- Avoid using email or other electronic means (e.g., text messages or instant messages) to transmit confidential case information.

Consider Implementing Any Applicable Evidentiary Privileges

To prevent third parties, including the subject of the investigation, from having access to the investigative materials, management should consider conducting the investigation under any applicable evidentiary privilege that provides the right to keep certain information from being disclosed without permission. That is, if an evidentiary privilege applies to information, the general rule is that the court and the party seeking the information will be denied access to it, and the triers of fact must disregard any evidence they do actually hear if it is deemed privileged afterward.

Legal jurisdictions, however, vary on which communications are protected by such privileges.

Typically, the most relevant types of evidentiary privileges for keeping investigations confidential are legal professional privileges. These privileges protect the communications between a professional legal advisor (e.g., solicitor, barrister, or attorney) and his clients, and in some situations, fraud investigations can be structured so that they are afforded protection

under such privileges. Generally, to receive protection under a legal professional privilege, an investigation must be conducted at the direction of, or under the supervision of, a legal professional.