# Chapter 41.
## Financial Forensic Services for Internal Investigations

## CONTENTS

1.0 Introduction .................................................................................................................. 825

2.0 White-Collar Crimes ..................................................................................................... 826
   2.1 Categories of White-Collar Crime ........................................................................... 827

3.0 Distinguishing a Financial Audit From Financial Forensic Services ......................... 827
   3.1 Differences Between Audit Procedures and Financial Forensic Investigation Methods and Techniques .................................................................................. 828

4.0 Indicators of Fraud ....................................................................................................... 831

5.0 Financial Forensic Services and Internal Investigations ............................................. 832
   5.1 Forensic Specialist Role in Internal Investigations ............................................... 832

6.0 Additional Internal Investigation Areas ..................................................................... 849
   6.1 Laboratory Analysis of Physical and Electronic Evidence .................................... 849
   6.2 Physical and Electronic Surveillance ....................................................................... 849
   6.3 Analysis of Financial Transactions ......................................................................... 849
   6.4 Processing, Sorting, Dissecting, and Drawing Conclusions From Data Gathered .............................................................................................................. 850

7.0 Common Mistakes in Internal Investigations ............................................................... 850
Chapter 41.
Financial Forensic Services for Internal Investigations

By Peter Resnick, CPA, CFF, CFE, and Greg Naviloff, CPA/ABV, CFF, CFE

1.0 Introduction
An internal investigation entails “the development and analysis of facts by an organization that will form the basis for a decision by the organization.” Federal enforcement agencies regard the existence of a comprehensive internal investigation process as a vital component of an effective compliance program. As such, properly scoped investigations conducted by qualified personnel can assist organizations with minimizing the risk of adverse enforcement actions, monetary penalties, and compliance obligations contained in any corporate criminal resolution. In addition, effective internal investigations help organizations identify the required course of action with respect to the underlying conditions that gave rise to the need to undertake such an investigation (e.g., financial statement restatement, disclosure to regulatory authorities, disciplinary action). The nature of those underlying conditions together with the possible implications for the organization will dictate the scope of an investigation as well as the need for specialized skills, such as those that financial forensic specialists provide.

Financial forensics (also commonly referred to as forensic accounting, forensic auditing, forensic investigation, or investigative auditing) refers to specialty accounting services used to identify and examine underlying facts in the context of internal investigations as well as dispute resolution (e.g., performing an economic damages calculation in a shareholder litigation).

The term “forensic” means “belonging to, used in or suitable to courts of judicature or to public discussion or debate … [and] relating to or dealing with the application of scientific knowledge to legal problems.” Financial forensic services “generally involve the application of special skills in accounting, auditing, finance, quantitative methods, certain areas of the law and research, and investigative skills to collect, analyze and evaluate evidential matter and to interpret and communicate findings.” As a general rule, financial forensic services represent a form of financial fact and evidence gathering, which is designed, prepared, and presented in a manner that will ultimately be deemed acceptable for use in the legal process.

---

1 “Internal Investigations,” Association of Corporate Counsel, Sponsored by Morrison Foerster, August 2012, p. 5.
2 Page 5 of “Evaluation of Corporate Compliance Programs—Guidance Document,” dated April 2019, issued by the U.S. Department of Justice Criminal Division, states: “Prosecutors should … assess the company’s processes for handling investigations of … complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.” justice.gov/criminal-fraud/page/file/937501/download.
4 Merriam-Webster online dictionary, merriam-webster.com/dictionary/forensic.
With this in mind, the discussion throughout this chapter recognizes broad categorizations that typically necessitate forensic investigations: (a) corporate internal purposes; (b) criminal investigation; and (c) civil litigation against an organization (e.g., shareholder or derivative suits). These are considered the three primary purposes of such work (“three purposes”). To undertake an effective investigation, it is important to recognize the applicable purpose from the outset to meet investigation objectives effectively and efficiently, including the development of a work plan that is inclusive of the expected procedures to be carried out (e.g., size and scope of the testing populations). This process is iterative in nature and will change as facts and circumstances change. The uncertainty or unknown is what gives rise to the iterative nature of an investigation. The various conditions of uncertainty cannot be readily captured in a single chapter of a handbook. An engagement may start as an internal corporate investigation but may expand into a criminal investigation involving federal authorities. Given the possibility of such variability, this chapter integrates the discussion on the three purposes, focusing primarily on the commonality of approach between them that can be pursued and occasionally highlighting items of peak interest that are specific to one of the three purposes.

Several commonalities of the three purposes of an investigation are addressed in this chapter. The first entails the identification, production, and safeguarding of relevant documents and data. The second is assembling an investigation team with professionals who have the requisite skill sets, training, discipline, knowledge, experience, independence, and integrity. The third commonality of the three purposes is striving to conduct a forensic investigation that follows the approach of inquiry, observation, and testing. Following such an approach should enable a forensic specialist to generate a work product that is verifiable, reproducible, and accurate, as well as serve as the basis for confirming or refuting any theories of events that were formed before the outset of the investigation. Financial forensic professionals who perform internal investigations often, among other things, have specialized knowledge about: (i) business information and financial reporting systems; (ii) generally accepted accounting principles (GAAP); (iii) evidence gathering, handling, and admissibility; (iv) investigative methods and techniques; and (v) litigation processes and associated protocols. In the pages that follow, each of these areas will be explained and discussed more completely. Within this chapter, we will provide an overview of:

- White-collar crimes and associated financial forensic services;
- The differences between a financial audit and forensic services;
- Indicators of fraud (discussed in further detail in Chapter 17);
- How to perform financial forensic internal investigation services (from engagement acceptance through conclusion);
- Specific considerations applicable to each financial forensic internal investigation; and
- Common mistakes to avoid when performing financial forensic internal investigation services.

### 2.0 White-Collar Crimes

Often, the financial forensic specialist is engaged to assist organizations with an internal investigation of white-collar crimes. The types of white-collar crimes are varied and numerous. However, the criminal statutes and their civil counterparts, and the intentional torts of fraud and conversion, can be summarized into a manageable number of categories.
2.1 Categories of White-Collar Crime
Exhibit 1 is a list of federal statutes that pertain to criminal fraud. This listing is illustrative only and not intended to be exhaustive.\(^7\)

These laws, combined with civil laws, create the legal causes for which financial forensic investigations are typically used.

White-collar crime is also described in the well-known occupational fraud survey titled “Report to the Nations on Occupational Fraud and Abuse,” published by the Association of Certified Fraud Examiners (ACFE). The ACFE Report to the Nations describes occupational fraud in three broad categories and quantifies their frequency and loss amounts. Exhibit 2 provides a brief summary of this information.\(^8,9,10\)

<table>
<thead>
<tr>
<th>Category</th>
<th>Prevalence</th>
<th>Loss Amount</th>
<th>Description</th>
<th>Example(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial statement fraud</td>
<td>Low</td>
<td>High</td>
<td>Occurs when there is a conscious effort by an employee(s) to produce financial statements with materially wrong accounting data</td>
<td>Timing differences, fictitious or understated revenues, concealed or overstated liabilities and expense, improper asset valuations and disclosures</td>
</tr>
<tr>
<td>Corruption schemes</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Occurs when an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer to gain a direct or indirect benefit</td>
<td>Schemes involving bribery or conflicts of interest</td>
</tr>
<tr>
<td>Asset misappropriation</td>
<td>High</td>
<td>Low</td>
<td>Occurs when an employee steals or misuses the organization's resources:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Theft of cash receipts</td>
<td>Skimming and cash larceny</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Fraudulent disbursements of cash</td>
<td>Billing, expense reimbursements, check tampering, payroll and cash register disbursements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Other</td>
<td>Cash on hand misappropriation and noncash misappropriation</td>
</tr>
</tbody>
</table>

### Exhibit 1. Criminal Fraud Statutes

<table>
<thead>
<tr>
<th>Criminal Violation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bankruptcy fraud</td>
<td>Title 18 USC</td>
</tr>
<tr>
<td>Computer fraud</td>
<td>Title 18 USC</td>
</tr>
<tr>
<td>Procurement fraud</td>
<td>Title 18 USC</td>
</tr>
<tr>
<td>Racketeer influenced and corrupt organizations statute</td>
<td>Title 18 USC</td>
</tr>
<tr>
<td>Bank fraud</td>
<td>Title 18 USC</td>
</tr>
<tr>
<td>Tax fraud</td>
<td>Title 26 USC</td>
</tr>
<tr>
<td>Tax shelter fraud</td>
<td>Title 26 USC</td>
</tr>
<tr>
<td>Management and financial statement fraud</td>
<td>Title 15 USC</td>
</tr>
<tr>
<td>Prohibited foreign trade practice (The Foreign Corrupt Practices Act)</td>
<td>Title 15 USC</td>
</tr>
</tbody>
</table>

### Exhibit 2. Occupational Fraud

3.0 Distinguishing a Financial Audit From Financial Forensic Services
It is important for the practitioner, as well as the intended audience of the practitioner’s work, to recognize that there are significant differences between audits performed to offer an opinion on the material accuracy of financial statements

---

\(^7\) “Forensic Accounting—Fraud Investigations Practice Aid 07-01,” AICPA, Appendix C.


\(^10\) ACFE “Report to the Nations on Occupational Fraud and Abuse—2020 Global Fraud Study,” p. 86.
and a forensic examination. Within the practice of public accounting, properly licensed persons (e.g., a certified public accountant, or CPA) perform defined assurance services under generally accepted professional standards (varying by geography and type of business), which typically culminate in a standard formal written report. One such assurance service is an audit. An independent external auditor performs work under the respective standards of the Public Company Accounting Oversight Board (PCAOB) and/or the American Institute of Certified Public Accountants (AICPA). Under these standards, an independent external auditor performing a financial statement audit “has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud.”

By contrast, while several professional institutions, each with their own standards, provide accreditation in forensic services, there are no unique licensing requirements for the provision of these services. In fact, financial forensic services are not by law or regulation restricted to being conducted by accountants. Furthermore, the objective of financial forensic services may vary for each engagement, although each one is generally designed to determine whether facts and evidence support or refute claims and allegations of fraud, waste, and abuse.

Besides these matters, there are significant differences between audit procedures and financial forensic methods and techniques.

3.1 Differences Between Audit Procedures and Financial Forensic Investigation Methods and Techniques

General Auditing Standards prescribe the requirements for a CPA to plan, conduct, and report the results of a financial statement audit. A number of the procedures the auditor uses to comply with the General Auditing Standards, together with the audit evidence the auditor relied upon, are identical or substantially equivalent to those a forensic specialist uses to perform financial forensic investigation services. However, audit methods, techniques, and procedures are by their nature designed to accomplish different objectives from financial forensic services. Much of the differences between financial audit procedures and a forensic investigation are the result of differences in scope and the application of procedures. A financial audit utilizes sampling to examine balances on a test basis to evaluate their characteristics, while forensic services may recompute entire populations of data, searching for patterns that may be indicative of a certain set of behaviors without regard to each event’s financial impact. The existence of the event that may prove fraud is, in itself, what is of importance, not specifically its size. The financial forensic specialists should be aware of these differing objectives and the need to design and employ appropriate methods, techniques, and procedures when performing financial forensic investigational services.

The significant differences between a financial statement audit and a forensic examination can be summarized as follows:

11 “The objective of the ordinary audit of financial statements by the independent auditor is the expression of an opinion on the fairness with which they present, in all material respects, financial position, results of operations, and its cash flows in conformity with generally accepted accounting principles.” Auditing Standards of the Public Company Accounting Oversight Board, Dec. 15, 2017, AS 1001.
13 For example, in July 2019, the AICPA released new professional standards for members who perform forensic services engagements. The Statement on Standards for Forensic Services No. 1 (SSFS 1) provides authoritative guidance for members providing litigation and investigative services. Specifically, the standards clarify the definitions of litigation and investigation, lays out key considerations for client and provider relationships, and establishes boundaries on the services members can provide.
14 Certain forensic services may be regulated by law, rule, or regulation (e.g., private investigative work).
15 General Auditing Standards consist of the general field work and reporting standards approved and adopted by the membership of the AICPA and amended by AICPA Auditing Standards Board and Public Company Accounting Oversight Board (the PCAOB). See Auditing Standards of the Public Company Accounting Oversight Board, Dec. 15, 2017.
16 “Audit sampling is the application of an audit procedure to less than 100 percent of the items within an account balance or class of transactions for the purpose of evaluating some characteristic of the balance or class.” Auditing Standards of the Public Company Accounting Oversight Board, Dec. 15, 2017, AS 1105, “Audit Evidence,” paragraph 28.
17 Appendix A to the AICPA’s special report “Forensic Procedures and Specialists: Useful Tools and Techniques” provides an excellent summary of the differences between GAAS audit evidence and forensic procedure evidence. The AICPA’s guide provides a practical comparison of GAAS audit evidence with forensic procedure evidence and discusses how forensic procedures differ from audit procedures.
Audits often culminate in a lower level of evidence gathering to form an auditor’s opinion and are often:

- Materiality-driven (testing focused on the concept of materiality\(^\text{18}\));
- Period-based (typically examining a fixed duration of time);
- Required (by contract, banks, U.S. Securities and Exchange Commission, legislative mandate, etc.) to assure compliance with accounting standards and company policy and procedures; and
- More broad (typically include comprehensive coverage of the complete entity).

By contrast, forensic examinations do not result in the issuance of an auditor’s opinion and are often:

- Exposure-driven (nonfinancial factors are often considered, such as an entity’s reputation and risk of litigation);
- Event-based (typically based on an alleged improper act); and
- More narrow (typically involve only those areas in which allegations exist).

As such, forensic examinations often require a greater level of evidence gathering. Some enhanced evidence-gathering procedures include:

- Public documents not necessarily considered during GAAS audits, including background checks;
- More in-depth interviews utilizing advanced techniques;
- Laboratory analysis of physical evidence to detect potential wrongdoing and/or analyze credible information (e.g., forensic technology specialist procedures and electronic and paper document review);
- More in-depth existence testing (e.g., authenticating addresses of a key party to a transaction);
- Electronic analysis/data mining (searching for unusual patterns and potential signs of fraud); and
- Supplemental investigative procedures with additional analyses appropriate for detecting specific fraud schemes.

As indicated earlier, while there is no required accreditation for forensic specialists and, as such, no single accepted authoritative standards for financial forensic services, a general consensus among financial forensics professionals has emerged as to the types of financial forensic techniques that might be employed depending on the circumstances. These techniques can be grouped into the following seven categories:\(^\text{19}\)

1. Public document reviews and background investigation (Section 5.1.3b)—By reviewing these types of records, a forensic specialist attempts to determine or understand possible motives (incentives and pressures) for perpetrating fraud. Information may be sought on key individuals, relationships, transactions, and organizations. The identification of activities, related-party transactions, or businesses of those under investigation is crucial to the identification of potential conflicts of interest.

\(^{18}\) "The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item." U.S. Securities and Exchange Commission Staff Accounting Bulletin 99—Materiality.

2. Interviews of knowledgeable persons (Section 5.1.3b)—This ordinarily should be a progressive process where forensic specialists obtain background information about the witnesses, the subject matter, and targets of an investigation. Each new interview should potentially result in new records and additional witnesses to interview. “Admission-seeking” interviews conducted of targets often include attorneys and an “Upjohn” warning.

3. Confidential sources—Forensic specialists may gain valuable information from the development of relationships and extraction of information from informants. While confidential sources can provide excellent information, forensic specialists can collect evidence from these sources that may be false. As such, professional skepticism dictates the need for corroborative evidence to reduce risk that hidden motives have resulted in inaccurate information. Additionally, it is important for forensic specialists to emphasize to their sources that absolute confidentiality cannot be assured.

4. Laboratory analysis of physical and electronic evidence (Section 6.1)—Forensic specialists may perform laboratory analysis to inspect credible evidence and analyze electronic evidence for indicators of fraud. In white-collar cases, these analyses may include a review for forged signatures and/or fictitious or altered documents and the use of computer software for digital imaging and data collection. Lastly, this category includes what is referred to as “data analytics,” a process of inspecting, cleansing, transforming, and modeling data with the goal of discovering useful information, informing conclusion, and supporting decision-making.

In its most basic form, data analytics may include the use of sorting and filtering tools and formulas (such as “if-then” and other logic statements) to analyze larger data sets to identify trends, anomalies, and/or transactions of interest. In more advanced application, data analysis can be used to perform complex pattern recognition, which can be automatically modeled using machine-learning techniques to provide exception reporting or identification of obscure relationships between multiple value fields in a large spreadsheet. Further, the use of effective data analytics techniques provides investigation teams with the ability to analyze the entirety of data available for a given scenario, and to look for connections or other unusual characteristics that may indicate fraud, enabling investigation teams to efficiently identify and target high-risk transactions for further examination.

Given the expansiveness of the topic of data analytics and its many benefits to corporate investigations, it could easily encompass the remainder of this chapter, so we have included a section titled “Common Analytical Techniques Used in Investigations” to provide greater context and examples of its potential use.

5. Physical and electronic surveillance (Section 6.2)—Law enforcement and private investigators often perform surveillance; however, a forensic specialist may utilize the technique. Examples include the monitoring of people, places, and objects, such as a loading dock after business hours.

6. Undercover operations—Law enforcement and licensed private investigators also often perform undercover operations. In most cases, forensic specialists would not participate in an undercover operation but might recommend that a client consider the technique. The forensic specialist may then utilize the information gathered in such an operation during the course of the investigation.

7. Analysis of financial transactions (Section 6.3)—Perhaps the techniques most commonly associated with a forensic investigation are the procedures a forensic specialist develops based on detailed knowledge of fraud schemes and indications of fraud. This knowledge is critical to developing tailored work plans and properly

---

executing the designed procedures. These techniques are performed to recompute, reperform, confirm, and/or substantiate the amount, timing, and business purpose of accounting transactions. Examples of procedures and techniques commonly used to detect fraud schemes are included in the sidebar.

Consideration and appropriate use of these techniques based upon the particular fraud risks associated with each organization and other circumstances are important in order for the forensic specialist to perform appropriate fact-finding associated with an investigation. Consideration of these techniques is useful when a specialist is seeking admission of his or her work for use in litigation because they provide the basic building blocks for compiling a thorough work plan.

In light of the significant differences outlined above between an audit performed under GAAS and the provision of financial forensic services, the financial forensic specialist should avoid using the terms “audit” or “review” in connection with services used for internal investigations. These two terms often refer to specific types of defined procedures and reports, and, therefore, their use by financial forensic specialists may create ambiguity.

4.0 Indicators of Fraud

The potential indicators of fraud are as numerous as are the scholarly articles devoted to their identification. There are numerous guides published to assist forensic specialists in identifying the specific indicators common to various types of fraud schemes. One such list can be found within Appendix A to AICPA's Business Valuation and Forensic & Litigation Services Section, Practice Aid 07-01, “Forensic Accounting—Fraud Investigations.” Additionally, some of these indicators are listed in Chapter 17, “Use of Forensic Evidence in a Lost Profits Case.” Additionally, the PCAOB and AICPA auditing standards, as well as “COSO Internal Control—Integrated Framework” (highlighted below), contain discussions of the elements of the well-established fraud triangle (pressure, opportunities, and rationalizations) and associated risk factors relevant to the detection of fraud.

2013 COSO Framework. The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control Integrated Framework (COSO Framework) was updated in 2013, the first revision since the original framework was published in 1992. The update included new principles that describe effective components of internal controls. Principle 8 specifically addresses that “[an effective] organization considers the potential for fraud in assessing risks to the achievement of objectives.” While most organizations integrate their assessment of fraud risk into their overall control risk assessment, the updated COSO Framework instructs organizations to give special attention to the potential for fraud and to discuss these risks with their audit committee.

An organization will most easily mitigate fraud risk by decreasing the opportunity to commit fraud; however, all components of the fraud triangle ought to be assessed within an organization. The risk of various types of fraud should be explored, and organizations ought to determine whether the controls in place would prevent or detect such frauds. As of December 2014, COSO does not recognize internal controls as effective without an organization’s compliance with the new principles.

21 Although forensic accountants may provide advice and recommendations concerning the specific procedures they might perform, an organization’s management makes decisions about, and is responsible for, the scope and sufficiency of the procedures. Cost/benefit and other considerations will preclude the forensic accountant from pursuing every conceivable source of information or performing every conceivable analysis.


23 The Committee of Sponsoring Organizations’ (COSO) mission is “to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.” COSO developed a “2013 Internal Control—Integrated Framework,” which sets forth the five components and 17 principles of an effective system of internal control. coso.org.

24 COSO “2013 Internal Control—Integrated Framework” sets forth the five components and 17 principles of an effective system of internal control. coso.org.
5.0 Financial Forensic Services and Internal Investigations

Prior to initiating an internal investigation, the appropriate stakeholders should decide how to handle and respond to complaints and allegations received. Internal investigations stakeholders often include those who are required to provide assurance as to the accuracy of financial statements (senior management and external auditors) as well as those with oversight and fiduciary responsibilities (general counsel, compliance officers, and audit committee members). A given organization should make the decision whether to perform an internal investigation, as well as setting the initial scope of the investigation, into known or suspected bad acts (improper conduct and/or violations of laws, rules, regulations, and policies) based upon an assessment of an initial allegation. As discussed later in further detail, it is a leading practice for every organization to establish a formal complaint-handling process to classify, evaluate, and investigate complaints.

Once this decision is made, appropriately defining the process and outlining the steps of the internal investigation will establish the integrity of the investigation process and improve the likelihood of fraud detection. A response should be thorough and properly executed to achieve a fair result and minimize risks to the organization and potentially to innocent parties. The investigation findings will likely include facts and circumstances, potentially responsible parties, any causal factors, appropriate responses, and any remedial actions necessary.

5.1 Forensic Specialist Role in Internal Investigations

Forensic specialists are widely used on investigation teams to gather and determine the relevance and reliability of financial evidence and to document findings. Common types of investigation engagements for forensic specialists include:

- **Investigation of suspected improper acts**—If the presence of a bad act, such as fraud, is possible but not certain (i.e., no specific allegations or very general allegations) and red flags or signs of possible improper activity exist, identification of risk areas should be performed and red flags or signs of possible activity should be explored. Often, investigation of suspected fraud results in broad-based procedures that cover a number of areas of an organization to assess whether additional or more detailed work may be required.

- **Investigation of assertions of improper acts**—In some instances, an individual may clearly and specifically assert bad acts such as fraud. In these instances, a more focused investigation is performed where techniques vary from assignment to assignment, depending upon the nature of the alleged act. This usually entails procedures in very specific areas to assess the accuracy and impact of the allegations.

- **Developing loss estimates**—This is typically conducted when an act is known to exist and believed to have resulted in damages. Often, an initial investigation has been completed. In estimating damages, the investigator usually assumes that the questioned acts or transactions are fraudulent, even though the ultimate conclusion of law regarding any fraudulent case is a matter for the trier of fact, if applicable. Loss estimates may be required for a variety of reasons including insurance reimbursement and sentencing purposes.

Regardless of the type of engagement, the basic steps necessary to complete forensic services for internal investigations generally include:

- Engagement acceptance;

- An initial allegation response (often performed by the investigation team before the forensic specialist accepts the engagement); and

- The completion of a fact-finding investigation (comprised of three phases: planning and communication, fact-finding and reporting, and concluding the investigation).

---

26 Examples would include an employee with a standard of living exceeding his or her earnings or an employee indicating an unnamed employee who may be misappropriating assets.
5.1.1 Engagement Acceptance
Forensic specialists, as a general rule, should have the experience and training to competently complete forensic services. They should be free of perceived conflicts of interest so they can complete their work with integrity and objectivity.

5.1.1a Conflicts of Interest
Financial forensic accreditation organizations, including the AICPA, have established professional guidance regarding conflicts of interest. Although forensic specialists may not be bound by such guidance because they do not hold such a designation, a forensic specialist who has appropriately addressed potential conflicts of interest should conduct internal investigations.

AICPA guidance indicates that “a conflict of interest may occur if, while performing a professional service for a client or employer, the [CPA] or the firm [employing the CPA] has a relationship with another person, entity, product or service that could be viewed ... as impairing the [CPA’s] objectivity.” When a perceived conflict exists, the CPA may still be able to perform the services. “If the [CPA] believes that the professional service can be performed with objectivity, and the relationship is disclosed to and consent is obtained from such client, employer, or other appropriate parties, the rule shall not operate to prohibit the performance of the professional service. When making the disclosure, the [CPA] should consider [AICPA] Rule 301, Confidential Client Information [ET section 301.01].”

5.1.1b Integrity and Objectivity
Another important component for a forensic specialist to achieve an effective internal investigation is to maintain both integrity and objectivity or impartiality. Commonly used definitions of these terms include:

Integrity—“To maintain integrity is to adhere to an ethical code and be free from corrupting influences and motives. The practitioner should not subordinate his or her judgment for personal gain or advantage when serving in a position of public trust.” Further, “integrity is measured in terms of what is right and just. In the absence of specific rules, standards, or guidance or in the face of conflicting opinions, a member should test decisions and deeds by asking: ‘Am I doing what a person of integrity would do? Have I retained my integrity?”

Objectivity or impartiality—“Impartiality is the innate ability to separate one’s self and self-interest from the investigation and its outcome” and can include “a trait that many consider neither to be a common trait or within human nature.” Fact-finders should not have any interest in the outcome of the investigation and should not allow one’s loyalty and self-interests to interfere with the fact-finding process or ultimate outcome. Further, “objectivity is a state of mind, a quality that lends value to a member’s services. It is a distinguishing feature of the profession. The principle of objectivity imposes the obligation to be impartial, intellectually honest, and free of conflicts of interest.”

According to the code of professional conduct AICPA established for its members, “in the performance of any [financial forensic] services, a member shall maintain objectivity and integrity, shall be free of conflicts of interest, and shall not knowingly misrepresent facts or subordinate his or her judgment to others.”

---

27 AICPA Code of Professional Conduct, Rule 102, “Integrity and Objectivity,” states: “In the performance of any professional service a member ... shall be free of conflict of interest.”
29 Ibid.
31 As stated in part by AICPA Principles of Professional Conduct ET Section 54 Article II.
33 As stated in part by AICPA Principles of Professional Conduct ET Section 5 Article IV—Objectivity and Independence.
As such, forensic specialists should carefully consider the impact of the following activities on their objectivity and impartiality:

- **Objectives of an internal investigation**—Although the forensic specialist may assist authorized decision-makers (typically the client) to decide the objectives of an internal investigation, the forensic specialist should not have the ability to make binding final decisions about objectives to avoid a potential conflict of interest by having a personally beneficial, vested interest in the outcome of the investigation.

- **Response and remediation**—Similar to the concerns above related to the objectives of an internal investigation, the forensic specialist should not have final decision-making authority related to the response and remediation of any adverse findings generated from the internal investigation. The fact-finders should have no say in the outcome because they should be independent from the decision-maker who will decide upon disciplinary and corrective actions. The decision-maker’s role requires conclusions regarding one’s actions.

- **‘State of mind’ issues**—The forensic specialist is not qualified to, and therefore should not, express any findings or opinions that involve the determination of any targets’ “intent” and/or “reliance,” which are “state-of-mind” issues.

- **Contingent fees**—The forensic specialist should not accept fees contingent upon findings or outcome, which may create a conflict of interest.

### 5.1.2 Initial Allegation Response

One leading practice for initially handling and responding to claims and complaints that might give rise to an internal investigation is to divide them into classes based on two broad sets of factors: sensitivity and materiality. The analysis of these two factors involves the assessment of both qualitative and quantitative risks.

- **Sensitivity:** This category includes factors that may cause financial harm to an entity if disclosed. Examples would include allegations of violations of laws, breaches of duty by senior officers or directors, and material internal control weaknesses.

- **Materiality:** This category includes factors that may have an impact on financial information (e.g., financial statements, regulatory filings, public disclosures, restrictive covenants, or incentive compensation) that could influence the economic decisions of the user of that information.

A complaint could be investigated depending on how an entity classifies it when it is received as part of a formal complaint-handling process. Specifically, the attributes of the complaint may determine which groups within and outside the entity may be involved. Based upon the two factors, claims can be classified as:

- Material and sensitive;
- Material and nonsensitive;
- Immaterial and sensitive; and
- Immaterial and nonsensitive.

The classification can assist in establishing the form and scope of an investigation team. Typically, if a complaint is found to be neither sensitive nor material to the financial statements, the entity’s board of directors can assign the investigation to uninvolved/disinterested management personnel and employees of the entity. For any of the other three
classifications of claims, one should consider the potential risk for an actual or perceived conflict of interest caused by the use of internal management personnel and employees to perform the investigation. As a general rule:

• Responsibility for overseeing an investigation should be given to an individual who is at least one level of authority higher than anyone potentially involved in the matter; and

• The board of directors or a committee of the board of directors should oversee the investigation of allegations related to senior management, with legal counsel appointed to supervise the investigation.

Some additional factors that might be considered as part of every investigation:38

• Urgency—An investigation may need to be performed in an urgent manner in order to limit losses and/or to protect evidence;

• Notification—Certain allegations may require disclosure to regulators, law enforcement, insurers, and/or auditors;

• Confidentiality—Information should be distributed only to those with a need to know;

• Legal privilege—Legal counsel should either lead or be involved as early in the process as possible to protect work product with attorney-client privilege;

• Legal and regulatory compliance—Investigations should comply with all laws and regulations, including those related to data privacy, information gathering, and interviewing witnesses;

• Securing evidence—Evidence should be collected and secured properly to protect the chain of custody and preserve admissibility; and

• Goals (objectives)—Specifics of the allegations should influence the investigation’s scope, focus, and timing.

5.1.3 Phases of a Financial Forensic Internal Investigation

Financial forensic services conducted (as well as the procedures performed) in connection with an internal investigation are specific to the facts and circumstances of each engagement. However, many investigations follow a typical process represented by three phases of work (see Exhibit 3). The first phase encompasses planning and includes, but is not limited to, the establishment of predication, project scope, communication protocols, evidence sources, and potential witnesses. Phase 2 involves fact-finding and analysis. Lastly, Phase 3 encompasses disciplinary or corrective action, reporting, response, and remediation (concluding the investigation).

<table>
<thead>
<tr>
<th>Investigation Team Member</th>
<th>Phase of Investigation</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Planning &amp; Communication</td>
<td>Fact-Finding &amp; Reporting</td>
<td>Disciplinary or Corrective Action</td>
<td>Remediation &amp; Prevention</td>
</tr>
<tr>
<td>Senior management</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Legal/compliance</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Investigation team (including forensic specialist)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Internal audit</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Human resources</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

5.1.3a Phase 1—Planning and Communication

The forensic specialist’s role during the initial phase should include:

- Establishing a team;
- Developing a work plan, which should include:
  - Tasks to be performed;
  - Assigning individuals to tasks;
  - Evaluation, documentation, and communication of useful/applicable information;
  - Identification of likely location of information; and
  - Conducting data gathering.
- Establishing control of an entity’s documents and files; and
- Developing a communication plan and lines of reporting.

As indicated earlier, the specific objective of an investigation is generally to gather sufficient relevant data to help the client or trier of fact reach a conclusion on the merits of the suspected or alleged fraud. To accomplish this goal, a fact-finder should consider the following items during the planning phase:

- **Determine proper predication**—Predication refers to fraud suspicions others have alleged. A summary of the predication should be provided to the forensic specialist and include an outline of the nature and background of the suspected or alleged fraud and basis for the belief. It is important to note that the forensic specialist’s role does not include the establishment of the investigation “objectives” of a forensic plan because this could be perceived to have an influence on the forensic specialist’s impartiality.

- **Conduct research**—Gain a thorough understanding of the background of the entity and relevant items, including industry norms, specialized accounting rules, and types of common fraud schemes for the industry/geography.

If additional indications of fraud are discovered beyond the scope of the initial assignment, the client should modify the understanding of the potential fraud and the scope of work via the execution of additional planning.

1. Establishing a Team

An interdisciplinary team with a relevant level of knowledge, skills, and experience should be assembled. Each team member has a specific role and involvement with certain phases of the investigation. Each investigation should be assigned a “leader” based on the nature of the investigation. Typically, the preferred way of assigning different groups to the investigation is based on the assessment of materiality, sensitivity, and industry experience. Preparing a plan, including identifying and qualifying experts, should be done as part of a comprehensive process (thereby having qualified resources available when needed). In many instances, it is not performed until a complaint has been tendered and an entity is under pressure to investigate.

2. Developing a Work Plan

Source and specificity of the allegation, and specific aspects of an entity’s control environment, generally influence the scope of work to be performed. However, it is desirable to be flexible when considering the initial selection of target accounts, entities, persons, etc., and to consider the following:
• Get buy-in from stakeholders on scope. In addition to those typically involved in corporate governance, stakeholders may include bankers, auditors, and regulators. For purposes of providing an opinion on the overall financial statements of the entity, the external auditors will need to understand the types of procedures being performed to gain comfort that the full extent of any fraud is identified. Only when the full extent of fraud is identified can the auditors quantify the financial impact and assess whether their previous opinion as to the accuracy of the financial statements needs to be withdrawn or altered.

• Scope should change if the investigation uncovers facts that should be further investigated.

• Scope should be clearly defined, and any changes should be easily traceable.

• Determine the extent of any statistical and nonstatistical sampling to be used.

Narrower scope—Generally, if a third party such as a government organization initiates the internal investigation, the investigation will be narrower in scope. The scope will be limited to the particular allegation of wrongdoing under investigation. For example, an inquiry from the U.S. Department of Justice may include specific allegations that an investigator will need to respond to in a timely manner.

Broader scope—If the investigation is entity-generated, meaning there has been no pressure from any third parties, the investigation may be broader in nature. However, the investigation team should still try to limit the scope of the investigation if possible (consider cost versus benefit). An entity does not typically use an internal investigation as a fishing expedition because substantial costs are involved in making an investigation broader than necessary. Therefore, the information-gathering process should be tailored to the particular allegation under investigation, especially when a well-developed compliance program has been established and internal controls are functioning as intended. In these instances, counsel can analyze the facts and decide upon the preferred strategy because there is no outside pressure from third parties.

2.1 Tasks to Be Performed
When evaluating tasks to be performed, it is helpful to go back to the seven techniques described in Section 3.1 and evaluate each to determine the appropriate method(s) to obtain the necessary information. Within sensitive areas of an investigation, information should be analyzed using multiple techniques (e.g., interviews and analytical testing). A helpful tool in developing appropriate steps in a work plan is to begin with the potential alleged scheme and consider the information that the trier of fact might feel is necessary. Also consider that, in some matters, intent or willfulness to defraud needs to be proven. A subject’s intent might be demonstrated by gathering evidence as to a scheme’s design, including evidence of premeditated plans, patterns of activity, and course of actions, including false and fraudulent pretenses and misrepresentations intended to obtain something of value. Work plans should, therefore, include steps to strive to document all aspects of a target’s actions (i.e., who, what, when, where, and how).

2.2 Assigning Individuals to Tasks
As discussed throughout this chapter, individuals assigned to perform discrete tasks should be given sufficient information to understand the purpose of the task and the expected outcome. When completing the task, the procedures performed should be well-documented and the work product should include the source of information used, scope of periods tested, and results.
2.3 Evaluation, Documentation, and Communication of Relevant/Necessary Information

A forensic specialist will often compile a formal document request list for circulation to the client and investigation team. A generic list of categories of documents required on typical investigations includes:

- Policy and procedures memorandums;
- Human resource files;
- Unconsolidated financial statement(s);
- Tax returns;
- Chart of accounts;
- Trial balance;
- General ledger activity;
- Journal entry posting report (with user ID and identification of manual entries);
- Subledgers for specific accounts related to alleged accounting issues;
- Account reconciliations related to alleged accounting issues;
- Relevant agreements with customers, suppliers, agents, and third parties;
- Underlying business documents for specific accounts related to alleged accounting issues (e.g., customer invoices, credit memorandums, vendor invoices, and purchase orders);
- Desk files and electronic spreadsheets maintained by targets; and
- Third-party records (e.g., bank statements printed directly from the bank website and vendor confirmations).

2.4 Identification of Likely Location of Information

In most instances, information will consist of paper and electronic records that are spread throughout the entity. Identification of the location of relevant information should be performed during and/or promptly after the distribution of a detailed request list. This process will also aid in quickly identifying any information that may not otherwise have been collected and preserved.

2.5 Conducting Preliminary Data Gathering

Preliminary data gathering assists the forensic specialist in gaining a general understanding of the type and size of issues and is the basis for assembling the initial work plan. The following list includes preliminary data-gathering steps that a forensic specialist should consider:

- Gain an in-depth understanding of the accounting/business process through the following steps:
  - Independent research (e.g., industry news and guides);
  - Review of financial statements; and
  - Review of policies and procedures.
- Interview whistleblower/complainant, if possible;
- Perform a walk-through of key transactions to better understand the typical process and controls; and
- Review electronic discovery plan. Evaluate the forensic technology specialist’s role, including plan and scoping of discovery and timelines. Assist with the identification of relevant custodians with relevant information and devices and documents that should be considered for collection. Provide first assessment of words to be utilized in a keyword search, if document review is being conducted.
3. Use of Forensic Technology Specialists

The collection of complete, accurate, and reliable electronic data, a need of most investigations, is beyond the skills of most financial forensic specialists, whose specialities lie within the areas of accounting and finance. As such, investigation teams should consider retaining a seasoned forensic technology specialist. The following list of steps is intended for forensic specialists to utilize to set objectives for a trained forensic technology specialist to assist in the proper and efficient collection of data (the subject of forensic technology specialists is extensive and, as such, is a potential chapter of its own): 39

- **Establish chain of custody**—A chain of custody is, in essence, a consistent trail showing the path of an item from the time it was acquired until the moment it is presented into evidence. 40 As such, in legal contexts, a chain of custody is the chronological documentation that records the sequence of custody, control, and transfers after information has been collected. Collection and transfer of original digital data to and between forensic technology specialist, forensic specialist, and other data custodians (even if for a brief period) should be included on a chain of custody document.

- **Determine the type of data to collect**—A variety of data types are likely either more or less relevant depending on facts specific to each investigation. The team should collectively evaluate which data types are of focus. Some examples of data types to consider include:
  - User-generated files such as emails, office productivity files (i.e., Microsoft Office files), PDFs, and scanned images (i.e., TIFF and fax);
  - Communications via email, text messaging, instant messaging, social media, collaboration sites, and voicemail or unified communications;
  - Internet activity including internet searches, browser history, etc.;
  - Data access, transfer or manipulation indicators; and
  - Accounting system data. 41

- **Determine the relevant data sources of data for collection**—A variety of data sources may contain information that is relevant to the investigative effort. The team should coordinate with the forensic technology specialists to determine the appropriate data sources that should be in scope for collection. Some examples of data sources that might be relevant include:
  - Computer systems such as laptops and desktops (whether physical or virtual);
  - Server data, such as:
    - File servers;
    - Collaboration server data such as SharePoint;
    - Enterprise resource planning (ERP) and general ledger (GL) software; and
    - Communications (i.e., email, internal instant messaging, voicemail);

---

41 Accounting systems data, in some instances, cannot be downloaded and accessed without a copy of the accounting system. Additionally, forensic technology specialists may capture accounting database tables that provide no context to the underlying accounting system (e.g., PeopleSoft, SAP, Peachtree). In some instances, the lack of context may limit the usefulness of the data obtained from the collection of this information.
Mobile devices; and

Cloud storage.

- **Determine where data are stored and maintained**—Data can be physically stored on devices or backed up remotely to servers (either in possession of the entity or outside parties). Forensic specialists and forensic technology specialists should work collaboratively with information technology professionals, operations, and other relevant data custodians to obtain an inventory of both the make and model of relevant devices and type of network(s) that the target of an investigation may have had access to. Such a list may include relevant flash drives, desktops, laptops, DVDs, mobile devices, shared network drives, etc.

- **Determine who has access to the data**—The forensic specialist will want to confirm that access logs and other relevant information are collected. The forensic technology specialist will often inquire with the investigation team as to the following:
  - What type of operating system is utilized?
  - Who has administrator rights?
  - Is there an access code?
  - When were the data (or systems) last accessed?

- **Collect and preserve data**—Devices collected need to be kept in an unaltered state. To accomplish this goal, plans should be developed to:
  - Preserve electronic evidence—Collect relevant data in a manner that will withstand scrutiny by the trier of fact; and
  - Properly store all electronic evidence—Both paper and electronic evidence should be properly stored to maintain appropriate chain of custody in the event regulatory inquiries or legal proceedings arise.

4. Establishing Control of an Entity’s Paper Documents and Electronic Files/Evidence

While paper documents and electronic files (collectively referred to here as “documents”) often form the foundation of the investigation, many clients tend to view document production as a burdensome and expensive irritant and often give retrieval efforts less than their full attention. Motive and intent are not typically identified strictly through accounting records but rather through personal communication between individuals, such as in email and other less formal communications (e.g., text messaging, instant messaging, social media platforms).

A review of documents frequently educates fact-finders or turns up information that helps unravel the wrongdoing. As such, documents relating to personal communication with others often provide the best record of the conduct.

To increase the amount of evidence available to investigators, safeguards should be employed to prevent the spoliation of evidence. Spoliation is the intentional or negligent withholding, hiding, alteration, or destruction of evidence relevant to a legal proceeding. For evidence to be admitted into litigation, a trier of fact will have to be convinced that evidence has been gathered lawfully and has not been altered. In addition, material evidence cannot be intentionally concealed,

---

42 Chapter 3, “Spoliation of Evidence,” of this publication includes further detail regarding this topic.

43 Black’s Law Dictionary.
withheld, or destroyed. A forensic specialist unfamiliar with acceptable practices is at risk of spoliation through unintended acts such as turning on a computer or reviewing electronic evidence without the data being properly preserved before the system or data is accessed, a process that typically involves the forensically sound processes and procedures.44

The following points should be considered when taking control of and reviewing documents and files:

- **Preventing documents from being altered, lost, or destroyed**—Even before the process of reviewing documents begins, legal counsel and its consultants should take action to prevent relevant documents from being altered, lost, or destroyed. Many organizations have in place a “legal hold” policy and procedures that require the identification and retention of relevant information when litigation is reasonably anticipated. A legal hold is a process that an organization uses to preserve all forms of potentially relevant information when litigation is pending or reasonably anticipated.45 As such, legal counsel, in coordination with the members of the investigation team, should focus on executing the entity’s document retention policy if one exists or otherwise develop and implement procedures designed to ensure that no documents are destroyed during the investigation.

- **Finding and reviewing**—As a preliminary matter, the investigation team leader should identify an employee(s) with knowledge of the entity’s paper documents and electronic files who will be in charge of retrieving relevant documents for the entity. A lawyer (either internal or external) should supervise that person(s). Systems should be put in place so that all potentially relevant paper documents and electronic files can be located.
  - For paper documents, this would include obtaining copies of the same document in different hands. This is important because some copies may have handwritten notes by the employees who received them. The investigation team leader should obtain detailed records of all of the locations in which paper documents are located. As documents are found, detailed records should be maintained as to where each paper document was located as well as where searches for documents were conducted.
  - For electronic files, which includes email, user files, and other relevant evidentiary information, it is critical to preserve the data first and then perform analysis from a copy of these data. If the electronic evidence is not preserved first, important information could be lost by simply opening a file, copying it to another storage media (i.e. USB drive, cloud storage), or printing the file.

- **Organizing documents**—When handling a document production, the investigation team should maintain the integrity of the original documents, while at the same time creating as few disruptions to the entity’s business as possible. A system should be developed for organizing documents. Lawyers generally create their own system, but a detailed privilege log should be retained separately from other documents to help avoid inadvertent disclosure.

5. Developing a Communication Plan and Lines of Reporting

A communication plan contains the entity’s plans for communicating key information to key individuals (e.g., the board of directors or special committee, external specialists, and management) from the outset of the investigation through
its completion. A robust communication plan is key to the effective execution of an investigation. Following are some of the leading practices to be agreed upon at the outset of an investigation:

- Establish an agreed-upon timeline, including key deliverables;
- Use a standardized reporting protocol to track details and status of the investigation and communicate with all members of the team accordingly;
- Agree on frequency of reporting;
- Establish a protocol (e.g., shared file on a server and weekly meeting) for tracking investigation progress;
- Agree upon lines of reporting and supervision, including:
  - To whom should investigation team members report;
  - Structuring of the forensic specialist’s reporting through legal;
  - Determining information flow; and
  - Frequency and direction of the reporting process (board of directors, client, forensic specialist, and general counsel).

5.1.3b Phase 2—Fact-Finding and Analysis

1. Evidence Gathering—Executing the Investigation Plan

One of the major objectives of a forensic specialist is to determine what will be done with the information that is obtained. As such, a forensic specialist should consider the relevancy of information as well as (in consultation with legal counsel as applicable) the standards of evidence a trier of fact, such as a court or tribunal, requires.

Upon identification of relevant information, the overall objectives of the investigation should translate into a specific work plan, which includes identification of documents and information to be analyzed and the performance of forensic procedures discussed in more depth later. The forensic specialist should also seek to identify possible logical alternative interpretations for the issues that have been identified (see “Reverse Proof” section).

The first step of the fact-finding phase, which should only commence after sufficient planning has been performed, is for the investigation team leader(s) to assign tasks to the appropriate team members. Tasks should be prioritized to perform higher-value procedures first (e.g., bribery allegations would first focus on accounting for cash balances and analyzing disbursements and customer refunds) and to organize tasks to reduce redundancy of work (e.g., it may be prudent to perform testing to identify suspicious vendors prior to running keyword searches for electronic document review).

2. Public Document Reviews and Background Investigation

External records can be a key component to investigations and may be overlooked by some forensic specialists.

The following types of information should generally be collected on targets of investigations to determine or understand possible motives (incentives and pressures) for perpetrating fraud. In many instances, this information is obtained as part of a comprehensive private investigator report.
• Personal information (relationships, lifestyle, etc.);

• Business and financial affiliations and associations;

• Litigation; and

• Personal assets, liabilities, and liens.

Examples of types of external third-party records that a forensic specialist may consider to corroborate internal records include:

• **Vendor information**—Confirmation of the vendor’s existence and procurement of an actual vendor invoice when a target is suspected of altering or creating fictitious vendor invoices;

• **Third-party inventory records**—Confirmation of inventory amounts purportedly held by external parties; and

• **Customer information**—Confirmation of the existence of customers.

3. Leveraging Forensic Technology

The reliance on electronically stored information is ubiquitous, and, as a result, the need to identify, preserve, and analyze that information is important to any investigation. The tools and techniques needed to properly collect and examine electronically stored information is becoming more complex and increasingly requires input from forensic technology specialists. Forensic technology specialists are often able to extract valuable information that can be used to inform the direction of an investigation. For example, forensic technology specialists who are engaged to capture and analyze electronically stored information are often able to quickly extract, summarize, and highlight relevant factual evidence associated with each custodian’s actions (e.g., password protection of files, deletion of emails or data, use of USB drives to remove/transfer data, use of special “wiping” software that permanently deletes data). Such information can be invaluable in determining: (i) who has something to hide; (ii) what people are trying to hide; (iii) what people are trying to destroy; (iv) what evidence is missing; and (v) the location of critical evidence. This information often provides a critical direction to financial forensic specialists at an early stage of the investigation.

4. Leveraging E-Discovery Tools

Once information is collected and processed (e.g., removal of redundant/identical information, conversion of characters into machine recognizable text, extraction of password-protected data), the resulting data can be ingested into electronic discovery, or “e-discovery,” software for searching, review, and tagging based on their relevancy. Forensic specialists often work closely with forensic technology specialists and document review teams to assist in utilizing professional judgment to uncover important documents and transactions using e-discovery tools and a controlled escalating review process.

Advances in e-discovery tools have greatly accelerated the process by which fact-finders are able to identify information relevant to the investigation. While broad-based “keyword” terms (words or combination of words, often within proximity of each other, typically associated with the issues being investigated) may be queried within the e-discovery data set to identify documents containing “hits” (documents that contain matching terms), many investigations now utilize dynamic review solutions that can expedite the document review process by employing a layered approach of filtering, analytics, text categorization, and validation that allow for the accurate identification and scoring of potentially high-value documents based on machine learning (thereby potentially reducing the number of documents that an investigation team reviews).
By working together, investigation teams can develop a wide variety of statistics to analyze the overall relevancy of the information reviewed (versus not reviewed). This information can be used to educate the investigation team as to the completeness of its review and the potential likelihood that additional information may exist that is not known to it.

Regardless of what methodology or tool is employed, it is important for investigation teams to document, from the outset, the instructions the system is provided (including any specific input on dates, custodians, words, other filtering criteria) and the machine-learning process employed. Documentation of the process the investigation team employed is essential so that, if needed, fact-finders can explain to the courts, other triers of fact, or other computer specialists the process utilized to identify and review a complete set of information potentially relevant to an investigation.

5. Interviews of Knowledgeable Persons

Arguably one of the most important tools for the forensic specialist is the interview process. Two of the more important keys to an effective interview include the style in which questions are asked and the clarity of the subject’s responses. Poor questioning style (such as the use of improper open-ended and closed-ended questions) can limit subject participation, and lack of clarity creates ambiguity, which makes assessing information difficult, if not impossible.

An inarticulate explanation may be caused by anxiety or may be the result of a subject attempting to evade answering a question. A forensic specialist should be able to control and direct the interview process to draw out further evidence and explore matters until satisfactory information is obtained. The styles and techniques needed to conduct an interview will change depending upon the type of subject (e.g., neutral third-party witness, corroborative witness, possible co-conspirator, and the accused), as well as the subject’s level of cooperation.

Additionally, forensic specialists conducting interviews should be familiar with the concepts jurors face, such as definitions of schemes to defraud and intent, prior to conducting interviews. These concepts can then be integrated into the questioning process for witnesses, victims, and suspects. Information obtained from an effective interview can help establish a pattern of deceit, cheating, and possibly lying that can be extremely useful in proving the intent to defraud.46

To conduct an effective interview, it is typically advisable to:

- Secure key documents in advance of the interview. Typically these documents will be organized by subject and/or in chronological order to facilitate identification; and

- Prepare an interview outline. Especially on more complex, larger investigations, the outline is a helpful tool to organize exhibits to be shown to the witness as well as key areas for follow-up or corroboration.

Determining order of interviews—Interviews can be ordered in a variety of ways. However, a forensic specialist typically will want to begin with someone in authority who is able to give an overview of the entity. In cases involving criminal investigations with third-party scrutiny, the primary target may be the second person interviewed. More typically, however, the next persons interviewed are those deemed to be the most cooperative and those who are least likely to be involved. Finally, those persons deemed to be less cooperative and those who were more involved are interviewed. This process increases the amount of relevant information and potential questioning prior to interviewing the primary target(s).

Structure of interviews—Interviews should be structured to protect attorney-client privilege whenever possible. It is important to caution employees not to discuss the interview with anyone else. Whenever possible, more than one interviewer should be present during interviews (a note taker who can also serve as a second witness). Notes taken should be in

---

46 AICPA Forensic and Valuation Services, section report, Conducting Effective Interviews, pp. 1-2.
the subject’s own words and include qualifiers (e.g., “about” and “I guess”), as well as the interviewer’s observations regarding large body shifts or behavioral change, and general story structure.

**Fact-finding or information-seeking interviews**—While there is no shortage of opinion on the best style and techniques of interviewing, the following list will serve as a helpful guide on the generally recommended steps for conducting an effective fact-finding or information-seeking interview. Key steps to an interview include:

- **Establish behavioral norm**—Establish an understanding of a subject’s normal behavior by observing verbal and physical behavior during nonthreatening moments and note physical (body position, gestures, and timing of changes) and verbal (upper and lower voice levels, speed of delivery, tone and language preferences) cues. These verbal and nonverbal behaviors will change as the subject’s anxiety changes in response to questioning. Typically, this step can be accomplished through verifying a subject’s personal background or through light conversation (e.g., “Tell me a little bit about yourself” or “Do you still live at …?”).

- **Establish your credibility**—This is done via an introductory statement and using a participatory and factual approach. Explain your role and explain how investigations are conducted.

- **Develop a rapport**—This is achieved by finding common interests or situations with your subjects through sharing personal information about yourself and asking about the individual (e.g., “Did you get any down time over the weekend?” or “Do you like golfing?”). It is also achieved by removing any perceived judgment (“I do want you to know that I am here not to measure the performance of your department, but to …”).

- **Reconstruct the circumstances**—After establishing the context of the investigation, ask the individual to reconstruct aloud the circumstances by including everything from appearance of scene, people present, weather, their feelings, etc. Ask the individual to include everything that happened from beginning to end, even if it seems unimportant.

- **Change perspectives**—Ask the individual to recall the incident from a different perspective (e.g., “recall events from end to beginning”).

- **Closing the interview**—Obtain additional biographical information, create a positive lasting impression, and encourage the subject to call you later with even a small detail that he or she remembers.

- **Detect indicators of potential lies**—The greater the fear of detection, the greater the likelihood of a change from a target’s normal behavior when lying. This change in behavior will reveal a subject’s deceptive status. When evaluating change in behavior:
  - Look for clustering of deceptive behaviors in response to questioning (changes in behaviors that occur in clusters of two or more); and
  - Disregard transient (isolated or individual) behaviors.
  - The greater the number of behaviors in the cluster, the greater the likelihood of deception.

**Admission-seeking interviews**—Admission-seeking interviews differ in that the goal of the interview is to obtain a verbal and, if possible, written statement from the subject (in his or her own handwriting) documenting his or her conduct without coercion. It should be noted that many interviews begin as information-seeking interviews and turn into admission-seeking interviews. Regardless as to whether the interview was initially conducted to obtain an admission, once an admission is sought, the interviewer will often focus on:
Providing rationalizations as to a subject’s conduct (giving him or her an excuse to minimize his or her conduct); and

Creating the sense of urgency (making him or her feel there is a limited amount of time).

These two key elements are useful in obtaining a target’s submission. Once submission is likely, assumptive questions are typically used to get the target’s admission, followed by answering the investigative questions of “who, what, when, where, how, and why.” The subject often memorializes these questions in a signed statement. Several seasoned interview-training organizations provide one-on-one intensive training sessions to forensic specialists to facilitate the mastery of these skills.47

Key Points to Every Interview

For a forensic specialist, an important element to an effective interview is knowing the facts of the investigation, which allows the interviewer to prepare thorough lines of questioning in advance of the interview and increases the opportunity for proper follow-up questions to an interviewee’s responses. The following list contains pointers for forensic specialists to consider in conducting interviews:

1. Potential conflict of interest warnings should be given to employees—a lawyer representing a corporation represents the corporate entity, not its employees. To avoid any confession, counsel will provide a warning to employees, often referred to as an “Upjohn” warning, whenever it is part of an employee interview.

2. Background and open-ended questions should be used at the beginning of the interview, together with a nonconfrontational review of documents;

3. Obtain the untainted story (the interviewer predominantly listens while the subject does the majority of the talking);

4. Closed-ended questions should be used to specifically explore an area of interest;

5. Avoid asking leading questions (e.g., “Was the account already overdrawn?”);

6. More contentious questions and a cross-examination style, if necessary, should be held off for later in the interview (if they are used at all);

7. Refrain from injecting one’s personal opinions into the interview or suggesting a theory or set of facts to an employee, either to help the employee recollect events or for any other reason;

8. Planting suggestions in an employee’s mind may interfere with discovering what really happened, not to mention that it may lead to charges of obstruction of justice;

9. Verify information obtained and reinterview subjects whenever necessary to clarify inconsistencies;

10. When necessary, use memory-jogging techniques (e.g., “Whom do they remind you of?”);

11. Avoid discussing the consequences of the subject’s actions or alleged actions; and

12. Employee rights during interviews vary based upon their type of employment (e.g., union employees, public employees, and at-will employees). When in doubt, legal counsel should be sought prior to conducting an interview.

47 AICPA and ACFE offer professional interviewing courses as do a number of specialized boutiques.
Memoranda of interviews—A memorandum of an interview should be prepared as soon as possible after an interview. A good rule of thumb is to strive to complete this within 48 to 72 hours. As time passes, recollection of details of responses not captured within notes diminishes quickly for most, resulting in a higher risk of incorrectly recalling pertinent information or confusing witness statements. The memorandum should identify any significant or hot documents presented and discussed during the interview.

Communication with former employees—It is not unusual for investigative counsel to interview former employees of the corporation. The opinion of the court in Upjohn did not address the issue of whether the attorney-client privilege extends to communications between counsel and former employees. However, in a concurring opinion, Chief Justice Burger noted his approval of a rule that would treat communications between counsel and former employees as privileged, including the typical situation where management asks a former employee to speak with a lawyer regarding conduct during the scope of employment.48

Addressing ethical concerns—It is important that employees feel confident that their comments will remain confidential to the extent possible. However, employees may incriminate themselves during the course of an interview, talking themselves out of a job or into the focus of a criminal prosecutor. Because of these issues, there is a potential conflict of interest between the fact-finder and employees. This risk becomes more significant when legal counsel participates in interviews. In these instances, to reduce later accusations of conflict of interest, written Upjohn transcripts are sometimes used. The transcript advises and warns the employee of the purpose of the interview, the employee’s rights and options, and the nature and extent of the confidentiality and privileged status that will attach to whatever is said in the interview. As discussed earlier, when counsel is involved, it often becomes important to make it clear to employees that an entity’s counsel does not personally represent them; attorney-client privilege belongs to the entity and not to the employee.

5.1.3c Phase 3—Concluding the Investigation

1. Concluding an Investigation
An investigation is a fluid process. However, the following are some general rules as to when an investigation should be concluded:

- Its outlined objectives have been met, and there are sufficient facts to make a credible determination as to what happened;
- The facts gathered are accurate and will enable the entity to reach a sound conclusion;
- Objectives have not been met, but continued investigation at the current time would not yield further information; and
- A governmental entity requested its conclusion and is conducting its own investigation.

2. Creating the Report
When legal counsel is supervising the investigation, it will determine the appropriate form of the report. Reports are drafted to include all relevant investigation findings (not just those forensic examinations performed).

Reports are often confidential and outside the reach of litigants. One of the purposes of reports is often to quantify losses. Loss calculations are performed within the context of an investigation’s purposes and, therefore, may not focus

on complete damage parties sustained. The most common omission being that investigation reports are often historical in nature and may not include potential future losses.

In addition to potential quantification of loss, reports should include discrete sections to allow the reader to easily follow work performed, facts obtained, and conclusions reached. Contents of the report may include:

- Client identity;
- Purpose of the investigation;
- Procedures performed during the scope of the investigation;
- Facts gathered during the investigation, including critical documents;
- Description of the participants involved in the activities of the investigation and their specific actions;
- Summary of findings;
- Recommendations for improvements to the control environment (if requested); and
- Limitations on the distribution of the report.

Forensic specialists should take careful steps to check that the contents of their report are accurate. The findings section may include a description of stated practices compared with the actual practices of individuals. In many instances, reports will contain quantification of improper conduct and both financial and economic impact on financial statements.

A report will provide factual findings that may identify the employees responsible for the wrongdoing and detail their wrongful conduct. In essence, the report will typically indicate that certain named employees of the entity may have violated policies or been dishonest. While the entity has an interest in deciding potential wrongdoing or criminal conduct, these employees may believe that their reputations have been harmed and decide to bring suit against the entity or even against those who wrote the report. A sample fraud examination report, along with other relevant sample fraud examination documents, is available on the ACFE’s website at acfe.com/sample-documents.aspx.

3. Determination and Communication of Disciplinary or Corrective Action

An effective investigation team should determine when it believes that the fact-finding effort is complete and the decision-makers have been provided with all of the information that is available.

The forensic specialist’s role in this process may include assistance with:

- Separating offenders (if more than one) into groupings of similar offenses; and
- Sorting offenders in each group by the extent of evidence against them.

After a review of the organizational policies regarding the matter in question, senior management, legal/compliance, and human resources should decide the appropriate discipline for each type of offense. Decisions by management are typically made after:
• Systematically matching the choice of discipline to the corresponding group of offenders in each grouping of offenses; and

• Reviewing the result for fair and equal treatment of each offender.

After a final determination is made on the form of discipline, decisions should be promptly communicated to appropriate parties. In some instances, an entity’s auditors and/or senior management uninvolved with the investigation will approach forensic professionals seeking sensitive information. Forensic specialists should take care to not divulge any sensitive information with those outside the investigation team without appropriate consent. Senior management and/or the legal counsel are typically those charged with informing auditors and any relevant government agencies, if necessary.

4. Remediation and Prevention

Effective investigation teams will leverage knowledge gathered throughout the investigation to improve policies and procedures, implement new practices, increase training on relevant policies, increase formal monitoring, and identify investigation leading practices/intellectual capital.

6.0 Additional Internal Investigation Areas

6.1 Laboratory Analysis of Physical and Electronic Evidence

As discussed in more detail in “Phase 1—Planning and Communication,” the collection of complete, accurate, and reliable electronic data is a challenge for many forensic specialists and will likely require specialized assistance to properly determine, among other things, whether evidence may have been destroyed or destruction was attempted. Separately, forensic specialists should document and make note of altered, fictitious, or forged documents during the course of their work, which may require further specialized analysis. Consult with an experienced professional when gathering and preserving these types of data to prevent spoliation of evidence.

Lastly, forensic specialists should work closely with data analytics professionals during the course of their work to assist with more complicated data extraction and data manipulation tasks that may be beyond their skill sets or may be more efficiently processed. Data analytics specialists who can be more adept at data manipulation can often more efficiently perform many of the “data-mining” procedures discussed in the exhibit “Common Analytical Techniques Used in Investigations” at the end of this chapter.

6.2 Physical and Electronic Surveillance

During the course of an investigation, engaging private investigators may be recommended to conduct surveillance of individuals to observe their activity and record their presence at various locations and times, including meetings with certain individuals. By having access to competent individuals providing surveillance services in a professional manner, a forensic specialist is able to provide more broad services to clients. Additionally, many states require special licensing to conduct this type of work, so it is important to determine whether any individual that is retained to assist is properly credentialed and qualified.

6.3 Analysis of Financial Transactions

Forensic specialists typically utilize financial analysis as a key tool during the investigation. The analytical process is not a simple one-size-fits-all exercise and is dependent on professional training in applicable areas such as accounting, audit, and exposure to and knowledge of many different types of fraudulent transactions. This background is essential to the prompt identification of problem areas (i.e., via analysis of red flags and suspicious patterns) and the creation of theories that can be tested. The forensic specialist should then properly refine the focus and/or refocus the investigation based upon the analysis of information received.
It is important to analyze the substance of a transaction and not just the form of the documentation of the transaction. To analyze the substance of a transaction, a forensic specialist should understand the business and the nature of the document being reviewed and evaluate the business reality or true business purpose.

See the box at the end of this chapter for a listing of some commonly used analytical procedures (this list is not intended to be all inclusive).

6.4 Processing, Sorting, Dissecting, and Drawing Conclusions From Data Gathered

Key information in processing, sorting, dissecting, and drawing conclusions from data gathered include determining:

- How long the activity has occurred;
- The financial impact of the activity;
- Who knew and when they knew;
- Actions taken post-awareness; and
- When to report findings to a higher decision-making authority.

Anomalies in data may not necessarily be indicative of improper or fraudulent activity. As a result, the forensic specialist should be cautious about forming opinions before an adequate investigation is complete. In any event, a forensic specialist should not offer any opinion about guilt or innocence because the ultimate conclusion of law is a matter for the trier of fact.

7.0 Common Mistakes in Internal Investigations

Unfortunately, even in well-organized, properly executed investigations, mistakes can be made. Mistakes typically are more likely made when there is:

- *Failure to include all relevant parties in the planning stage*—When possible, members of an investigation team should have early communication and “buy-in” on procedures from oversight authorities and external accountants. “Redos” can significantly increase the cost and length of the investigation and may not always be possible.

- *Improper selection of investigation team*—Proper due diligence of the members of an investigation team is essential. When the investigation team is inadequately selected, internal and external decision-makers do not typically realize that they do not have sufficient facts to make decisions until after fact-finding is complete. In some instances, the poor quality of work is not known until after action has been taken.

- *Inadequate initial response*—When the target of the investigation is not isolated and restricted from accessing potential evidence on a timely basis, there is a significant chance of evidence destruction.

- *Improper or inadequate collection and analysis*—This is perhaps the most challenging and highest risk area for most forensic specialists because the prevention of mistakes relies on the thoroughness of procedures based upon the experience and training of the professionals. Some common mistakes forensic specialists should be concerned with include:
Lack of consideration of data privacy laws—This often occurs either when there is an inadequate review of an organization's privacy policy or inadequate consideration of relevant data privacy laws and regulations. An organization's privacy policy should be reviewed, and collections should be performed under the guidance of knowledgeable legal counsel to confirm that evidence has been collected in accordance with that policy and applicable laws.

Lack of establishing the chain of custody—This often occurs either when documents are not treated as if they are subject to applicable rules of evidence. Proper chain of custody should be maintained from the outset to preserve admissibility, particularly in instances in which litigation is likely.

Inadequate document review—Performing a full review of relevant documents often requires the use of electronic search tools. Use of unsophisticated search tools when conducting document review can result in incomplete reviews. For example, certain file types (e.g., scanned PDFs and password-protected files49) should be properly processed to convert files into text searchable documents. Additionally, the use of overly narrow search terms or search terms that are not properly vetted can result in the reperformance of work (at the request of outside stakeholders such as regulators and auditors) or result in an investigation with incomplete evidence for evaluation by the trier of fact.

Improperly conducted interviews—Interviews that are conducted too early in the investigation process, improperly documented, or conducted by poorly trained interviewers can lead to inefficient investigations. Forensic specialists should have a plan as to the order in which interviews are conducted. Typically, interviews are more useful when a sufficient amount of documentary evidence has been obtained and key facts (i.e., chronology of events, complete population of suspected transactions, likely motives of the target, etc.) are known beforehand. Information obtained from interviews of witnesses is often valuable when interviewing targets. Additionally, poor note-taking can lead to the need for additional interviews to confirm statements as well as potential reliance on false or inaccurate information. Utilizing two individuals during interviews, as well as prompt memorialization of interview notes, can reduce this risk. Lastly, untrained interviewers are more likely to miss significant nonverbal behavioral changes and less likely to use appropriate types of questioning to conduct an effective investigation. The note-taking role provides a good opportunity for less-seasoned interviewers to learn these skills.

Errors in analyses—A variety of errors can occur when analyzing data. Perhaps the most common of these errors includes the utilization of duplicate data/transactions (double counting) as well as inappropriate sampling methodologies. When evaluating data and potential damages/losses, a forensic specialist should be as specific as possible, avoiding broad categorization of issues, which can result in the inadvertent double counting of errors/issues. Additionally, when developing samples, forensic specialists should exercise caution when extrapolating losses based upon a nonstatistical sample. While nonstatistical, risk-based sampling that is considered representative of key behaviors within a population can be useful, samples that are haphazard may have little value in drawing conclusions about a data population as a whole or in finding actual results of system failures. Samples should typically be obtained to achieve a 90%-to-95% confidence interval. Sampling errors increase and decrease as a function of how many of the population members are sampled, as well as the homogeneous nature of the items being sampled.

Overreliance on regression analysis to conclude upon relationships—Regression analysis includes techniques for modeling and analyzing relationships within data (between a dependent variable and one or more

49 The investigation team should generate and evaluate a listing of password-protected files. Where files are deemed to be potentially relevant, those files should be broken or cracked, if possible.
independent variables). The analysis can be used for prediction and forecasting, which often makes it a helpful tool. However, forensic specialists should use caution when utilizing small sample sizes. While it is tempting to rely upon small sample sizes when data are limited, the information obtained from such analysis is often of limited use.

- *Untrained use of statistical concepts*—Statistical samples can be improperly used by untrained users and can unintentionally provide false results. Forensic specialists should understand statistical variables used in their findings and, when in doubt, consult a statistician.

In conclusion, the forensic specialist’s skills and competency can impact the effectiveness of a financial investigation. Forensic specialists should strive to master the knowledge and concepts discussed in this chapter, gain experience in identifying the telltale signs of the multitude of fraud schemes, become skilled in identifying relevant information and making the best use of that information, and become experienced documenting and communicating relevant factual findings to stakeholders.
Common Analytical Techniques Used in Investigations

• **Chronology of events and fact sheets**—When performing more in-depth forensic investigations, it may be prudent to turn simple chronologies into more of a visual representation of the information gathered during background research, interviews, and surveillance (sometimes referred to as a network diagram). Gathering this information in one place allows a forensic specialist to evaluate patterns of activity and identify other entities and parties meriting further investigation.

• **Net worth or modified net worth method**—This method is a common tool, which dates back to when the IRS used it in its conviction of Al Capone. As such, courts have accepted this as admissible circumstantial evidence. This technique is effective in demonstrating apparent income by determining the increase in one’s wealth. The calculation is typically performed as follows:

1. **Identify** increased net worth by comparing period-end net worth estimates for two consecutive periods;

2. **Add** the results from Step 1 to known living expenses; and

3. **Subtract** the income from known sources of income.

The residual amount calculated at the completion of Step 3 identifies the period-to-period change in expenditures in one’s overall net worth in excess of the known sources of funds.

• **Cash sources and uses**—This method lists each identified source and use of cash (or other funds) by category for the respective years under analysis. This method is similar to the net worth method and is often used interchangeably. In many instances, living expenses for the respective years are partially derived from adjusted third-party information sources such as the Consumer Expenditure Surveys available at bls.gov/cex/home.htm.

• **Proof-of-cash method**—The proof-of-cash method is utilized to isolate and identify specific unrecorded transactions. It seeks to prove that all the receipts and payments obtained from banking records are consistent with all the receipts and payments in the cash receipts and disbursements journals. This method is useful for uncovering schemes where employees attempt to misappropriate cash by not recording bank deposits and expenditures on the general ledger. To accomplish this test, a forensic specialist will begin by comparing the following balances on bank statements and general ledger reports:

  o **Beginning balance**;
  o **Cash receipts**;
  o **Cash disbursements**; and
  o **Ending balance**.

Variances between the bank statement balance and book balance should be investigated. Typical differences should only include timing differences between receipts and disbursement posting dates between the two sets of reports, which are easily confirmed via review of prior and subsequent period statements/reports.

• **Sampling techniques**—During the planning phase of an investigation, the forensic specialist should thoroughly evaluate the pros and cons of utilizing sampling. Sampling is one of the most common
techniques used to both narrow the time period investigated and efficiently and economically estimate the losses injured parties incurred. Sampling, when employed properly, may utilize statistical reliability to give a level of confidence that can closely match a more expensive and time-consuming investigation. As such, forensic specialists should determine the appropriate method after considering their relative cost and effectiveness in conjunction with the specific circumstances of each investigation.

Sampling is beneficial and may be used when there are sufficient records supporting transactions. Examples of transactions that typically permit sampling include: sales entries (to evaluate existence), sales returns (to evaluate the existence and/or frequency of cash refunds, typical of bribery and other schemes), and overstatement of assets (to evaluate appropriateness of capitalization). However, in many instances, sampling is not possible, such as when transactions are not recorded through the financial statements or are inadequately documented or incomplete (as may be the case in skimming and cash theft schemes).

Before employing sampling techniques, significant consideration should be given to the ultimate use of the investigation results. To the extent it is likely that findings will be presented to a jury, there should be consideration of the level of confidence that the specialist is likely to achieve, the risk associated with convincing a jury of the mathematical certainty, and the likelihood that the method will withstand cross-examination.

- **Attributes sampling**—This sampling type is often used to determine whether an item being sampled does or does not contain certain characteristics or attributes. The test is performed to determine how many times a certain attribute will occur in a population. As such, this technique is commonly used to test internal controls. In attributes sampling, each deviation from a prescribed control is given equal weight in the sample evaluation, regardless of the dollar amount of the transactions. Forensic investigation may utilize this method to test the rate of deviation (or error) from an expected control in order to support the forensic specialist’s assessed level of substantive procedures. For example, suppose the sample consists of 50 sales credits issued and company policy requires all credits over $100 to receive authorization from a supervisor. If your analysis indicated three of the 50 items are not properly approved, the implied population error rate is 6%. This error rate’s acceptability would be based on the forensic specialist’s assessment of tolerable error, expected error, sampling risk, and confidence interval.

- **Variable sampling**—If the objective is to obtain evidence directly about a monetary amount being examined, the forensic specialist generally designs a variables sampling approach. With a variable sample (as with an attribute sample), forensic specialists treat each individual item in the population as a sampling unit. Forensic specialists will use this method to evaluate the entire population based on selected sample data. Forensic specialists commonly use three types of variables sampling estimators: mean per unit, ratio, and difference.
  - **Mean per unit**—As the name implies, this method utilizes the mean. Forensic specialists can use this method to evaluate characteristics of the total population being examined. Taking the average value (i.e., the mean) of sampled items permits the estimation of the true population value. As such, the mean-per-unit method is a useful tool to consider when a forensic specialist does not have a complete set of underlying documents to support an account balance.

    For example, if a forensic examination includes a population of 1,200 invoices in accounts receivable and the sample size consists of 40 invoices with a total value of $1,000 and a mean of $25 ($1,000/40), using the mean-per-unit method, the estimate of the total value of accounts receivable in the population is $30,000 ($25 × 1,200). After analyzing variation in the sample and specifying a desired confidence interval, the forensic specialist can provide a statistical estimate of the account balance (e.g., if a forensic specialist’s
desired confidence interval is 95%, then, after assessing the variability of the invoice amounts in the population, the forensic specialist might conclude he or she is 95% confident that the total value of accounts receivable is $30,000, ± $3,000).

- **Ratio**—This method applies the sample ratio across the entire population to calculate an error amount. For example, suppose a forensic specialist’s accounts receivable sample contains errors totaling $50 on total claimed accounts receivable of $1,000. The error rate is 5% ($50/$1,000). By applying this same rate to the entire population, the forensic specialist could extrapolate the projected dollar amount of errors within the entire account balance. Continuing with this example, if total accounts receivable in the population is $40,000, then the extrapolated error amount is $2,000 (5% × $40,000).

- **Difference**—This method calculates the average difference between a reported result and the corrected amount for a sample of observations (for example, an average overcharge or other average error amount). This average difference is then multiplied by the total number of observations in the population to extrapolate the total population difference or error. In our previous example, the forensic specialist’s population included 1,200 items and forensic sampling procedures identified errors totaling $50. If the sample consisted of 50 items, the projected misstatement using the difference estimator would be $1,200 (($50/50 sampled items) × 1,200 population items).

- **Stratified sampling**—While forensic specialists should be familiar with many useful statistical sampling techniques (simple random, systematic, and probability proportional to size), stratified sampling is perhaps the most important. The stratified technique is used to improve the accuracy of a standard sampling technique without increasing the sample size. The technique uses stratification of the population and samples each stratum separately. The advantages of this sampling include the ability to:
  - Test hypotheses and draw conclusions about specific subpopulations;
  - Use different techniques for different subpopulations; and
  - Improve the accuracy/efficiency of estimation.

- **Reperformance**—The forensic specialist will often reperform accounting procedures and calculations by the organization that he or she is investigating. Reprocessing permits a forensic specialist to assess and potentially confirm a transaction or account balance’s accuracy and existence (e.g., bank reconciliation) and may provide a reference point for further investigation testing procedures. To the extent the use of judgment is required within a calculation, such as is typically the case when valuing an organization’s reserve accounts, the forensic specialist should evaluate all relevant business considerations, establish a rationale and reasoning for application of facts most relevant to the estimation, and carefully document all underlying assumptions along with applicable support.

- **Data-mining procedures**—Data mining, or data analysis, can streamline investigations that involve a large number of transactions. Even smaller organizations are capable of conducting tens of thousands of transactions. Quickly narrowing the population to a more manageable size to identify those with potentially inappropriate or illegal purposes can be difficult. Tools such as Benford’s Law (described more fully in the next section) as well as many nonstatistical data analysis tests can be utilized to identify unusual transactions and potentially narrow the scope of transactions to be reviewed. The following is a short list of frequently used data analysis tests:
Different vendors at the same address;
Payments to customers;
Gap analysis in data ranges; and
Missing or omitted data fields.

The creation of these tests is only limited by the forensic specialist’s imagination. Many digital forensic libraries are available to help forensic specialists identify useful tests that can be tailored to their investigation. Perhaps the most efficient starting point for all data-mining exercises is for the forensic specialist to evaluate the usefulness of all available system-generated exception reports.

- **Benford’s Law**—Benford’s Law states that digits and digit sequences in a dataset often follow a normally distributed predictable pattern. The Benford technique analyzes data sets for possible errors, potential fraud, or other irregularities via the identification of deviations from these predictable patterns of digits. Examples of patterns that one would expect this analysis to identify would include unusually high numbers of journal entry postings at an unusual time or date and disbursements of round dollar amounts, etc. If improper entries are posted in sufficient quantities, then these artificial values contained within a larger dataset will skew the distribution of the digits in the dataset, creating a pattern, when viewed graphically, that is different from the one Benford’s Law predicts.

- **Reverse proof**—The examination of forensic investigation matters should be evaluated from two perspectives and include attempts to prove:
  - That a fraud (or other deceit) has occurred; or
  - That a fraud has not occurred.

The reason for reverse proof is that both sides of fraud must be examined. Under the law, proof of fraud must preclude any explanation other than guilt. By thoroughly investigating other potential explanations, a forensic specialist provides the best possible facts to those charged with evaluating guilt.

- **Analytical review of financial statement balances (including common sizing and ratio analysis)**—This procedure will often include the calculation of period-over-period changes in accounts (horizontal analysis), common sizing (vertical analysis), and ratio analysis to better understand the causes of changes within financial statements.

  With each of these tools, the forensic specialist will first develop an expectation of the direction and magnitude of change in a key account or ratio and compare the expected change to the actual change. Any discrepancy between expected and actual changes should be investigated. For example, when reviewing an accounts receivable balance, a forensic specialist will have evaluated the accounts receivable aging and the sales volumes immediately preceding each balance sheet date to develop an expectation of whether the accounts receivable balance would have been likely to increase or decrease. Bar graphs and line charts are useful to identify key variations warranting further investigation.

  In a basic horizontal analysis, a relevant base period is identified and the dollar amount of each financial statement item in subsequent periods is converted to a percentage of the base year dollar amount. Often comparing key account categories (e.g., travel, entertainment, reserve accounts, and officer compensation) over a multiperiod time horizon will reveal patterns meriting further investigation. This may also include the
Chapter 41. Financial Forensic Services for Internal Investigations

comparison of an entity’s own performance over a period and/or a comparison with industry benchmarks or those of specific competitors.

Common sizing consists of converting all financial statement items to a percentage of revenue and assets and then comparing the results within and among one another over a multiperiod time horizon. This method enables a comparison to similar businesses that may be of different sizes. Variation from normal growth within the industry or from competitor averages would be evaluated for reasonableness, and the potential causes would be evaluated further.

Lastly, ratio analysis in the hands of a forensic specialist can provide both quantitative and qualitative information about an organization’s financial statements.

Ratios are calculated using relevant base periods and then compared to other periods, companies, the industry, or even the economy to analyze the performance of the organization and identify anomalies. Some useful ratio analyses used in detecting potential earnings management include:

- **Cash realization ratio (CRO)** = \( \frac{\text{Operating cash}}{\text{Net income}} \)

  As the ratio suggests, CRO measures the ratio of operating cash flow relative to net income in a given period. Analyzing this ratio from period to period, particularly on a quarterly basis, can highlight variations that may suggest earning management. Artificial smoothing earnings over financial reporting periods does not typically impact cash flow. As such, unexplained fluctuations between the level of cash flow from operations and net income (after reconciliation for specific items such as depreciation and amortization) could suggest that net income is being managed.

  Note that the ratio will usually be less than 1.0 but is highly dependent upon industry. Operating cash as a component of net income may rise over time, although significant volatility from period to period should be investigated further.

- **Asset quality index (AQI)** = \( \frac{\left(1 - \frac{\text{Current Assets}_t + \text{PPE}_t}{\text{Total Assets}_t}\right)}{\left(1 - \frac{\text{Current Assets}_{t-1} + \text{PPE}_{t-1}}{\text{Total Assets}_{t-1}}\right)} \)

  The above AQI formula measures the ratio of noncurrent assets other than property, plant, and equipment (PPE) to total assets where “t” represents a specific period being analyzed. AQI measures the ratio of asset quality between period “t” and prior period “t - 1” and is useful in quantifying the proportion of total assets for which future benefits may be less certain. If the AQI ratio is greater than 1.0, it indicates a potential increase in cost deferral and, as such, may indicate a greater likelihood of earnings manipulation.

- **Depreciation index (DI)** = \( \frac{\text{Depreciation}_{t-1}}{\text{Depreciation}_{t-1} + \text{Net PPE}_{t-1}} \) / \( \frac{\text{Depreciation}_t}{\text{Depreciation}_t + \text{Net PPE}_t} \) \)

  The above DI formula calculates the ratio between the rates of depreciation for period “t” with prior period “t - 1.” The depreciation rate is comprised of depreciation expense and net PPE. A DI greater than 1.0 suggests that the rate of depreciation has slowed, thus indicating changes to estimated useful lives or new methods. Therefore, one can generally expect a positive relation between DI and the probability of earnings manipulation.
The Comprehensive Guide to Economic Damages: Volume One

- **Days sales in receivables index (DSRI)**
  \[
  \text{DSRI}_t = \left( \frac{\text{Receivables}_t}{\text{Sales}_t} \right) / \left( \frac{\text{Receivables}_{t-1}}{\text{Sales}_{t-1}} \right)
  \]
  The above DSRI formula calculates the ratio of days sales in receivables for period “t” with prior period “t - 1.” This ratio can be useful in evaluating whether receivables and revenues are out of balance in two consecutive periods. When DSRI is less than 1.0, receivables as a ratio of sales have decreased over time, which may be indicative of manipulation of sales.

- **Gross margin index (GMI)**
  \[
  \text{GMI}_t = \left( \frac{\text{Sales}_{t-1} - \text{CGS}_{t-1}}{\text{Sales}_{t-1}} \right) / \left( \frac{\text{Sales}_t - \text{CGS}_t}{\text{Sales}_t} \right)
  \]
  The above GMI formula calculates the ratio of gross margin (i.e., sales less cost of goods sold (CGS)) for period “t” with prior period “t - 1.” When GMI is greater than 1.0, gross margin has deteriorated, which could indicate earnings manipulation. On the other hand, GMI less than 1.0 could indicate skimming of receipts.

- **SG&A expenses index (SGAEI)**
  \[
  \text{SGAEI}_t = \frac{\text{SG&A Expense}_t / \text{Sales}_t}{\text{SG&A Expense}_{t-1} / \text{Sales}_{t-1}}
  \]
  The above SGAEI formula calculates the ratio of SG&A expense for period “t” with prior period “t - 1.” A SGAEI of greater than 1.0 can indicate sales increased faster than associated selling expense, which could potentially indicate earnings manipulation if sales growth is unexplained (e.g., no significant acquisition or expected growth).

- **Total accruals to total assets (TATA)**
  \[
  \text{TATA}_t = \frac{\text{Current Assets}_t - \text{Current Liabilities}_t - \text{Cash}_t - \text{Current Long Term Debt}_t - \text{Income Taxes Payable}_t - \text{Depreciation & Amortization}_t}{\text{Total Assets}_t}
  \]
  TATA is comprised of the change in working capital, less cash and depreciation/amortization. Changes in this ratio from period to period may indicate earnings manipulation resulting from management accrual decisions, particularly short-term decisions. Higher positive accruals (excluding cash) are generally correlated to a likelihood of earnings manipulation.

- **Journal entry review and subledger reviews**—In many financial fraud investigations, a forensic specialist will review various types of suspicious journal entries and transactions. Once journal entries and subledgers are obtained electronically, suspicious transactions can sometimes be easy to detect through the use of tools such as data mining or Benford’s Law, discussed previously. Some inherently risky journal entries that a forensic specialist may want to consider include:
  - Journal entries senior management made, typically referred to as “top-side entries” or “manual entries,” to adjust reserves and financial statements as part of the financial closing process. When properly recorded, senior management fully documents these journal entries with a clear and reasonable business purpose.
  - Journal entries posted between unusual account combinations (e.g., credit entries to expense accounts), which can be attempts at concealing improper activity.
  - Journal entries made at unusual times (e.g., late in the evening or on a weekend, depending on the company’s operations) or posted by unusual or unauthorized users.
About Business Valuation Resources

Every informed stakeholder in business valuation, performance benchmarking, or risk assessment turns to Business Valuation Resources (BVR) for authoritative deal and market data, news and research, training, and expert opinion. Trust BVR for unimpeachable business valuation intelligence. BVR’s data, publications, and analysis have won in the boardroom and the courtroom for over two decades.

Deal & Market Data

- DealStats
- Cost of Capital Professional
- Valuation Benchmarking Platform
- Guideline Public Company Comps Tool
- BIZCOMPS
- Economic Outlook Update
- FactSet Mergerstat/BVR Control Premium Study
- Stout Restricted Stock Study™
- Valuation Advisors Discount for Lack of Marketability Study
- ktMINE Royalty Rate Data & License Agreements
- First Research Industry, State & Province Profiles
- BizMiner Industry Financial Reports
- Mergerstat Review & Mergerstat Review Monthly
- Butler Pinkerton Calculator – Total Cost of Equity and Public Company Specific Risk Calculator
- Vertical IQ - U.S. and Canada Industry Profiles
- RCRReports

Guides, Books & Reports

- Digital Library
- Guides & Books
- Special Reports
- Legal Compendiums
- Yearbooks

Training & CPE

- Webinars
- Web Workshops & Special Series
- Desktop Learning Centers
- Self-study CPE
- eLearning courses

News & Research

- BVResearch Pro
- Business Valuation Update
- BVLaw
- Economic Outlook Update
- Business Reference Guide Online

Learn more about all of our offerings at: bvresources.com