CHAPTER ONE

F – Forgetting the Present and the Past

Accounting Humor

Q – What is an accountant?
A – Someone who solves a problem that you didn't know existed, in a way you don't understand.

IN THIS CHAPTER, WE discuss the landscape of the global ethical environment, and then establish the professional standards that help address the dilemmas that arise out of fraud and misconduct. We compare financial statement audits and fraud investigation from the perspectives of auditors and fraud examiners.

FRAUD IN THE PRESENT AND PAST

I challenge you to grab a periodical. A newspaper (if you are still able to stomach the news). Scan it. How many articles mention fraud or misconduct? I would be willing to wager each issue has a few. I would also be willing to bet that each victim represented in the article strongly felt that "it could never happen to us." We, as accountants and auditors, are not immune. We are lulled into a false sense of security, and feel that our clients or companies "are better than that." This is very apparent in recent studies on the impact of fraud on small business. In fact, the Association of Certified Fraud Examiners 2018 Report to the Nation showed that small organizations with less than 100 employees are mostly likely to suffer from occupational fraud (28% of cases) and suffered the largest median loss (USD 200,000).

It *can* happen to you. I know, because it happened to me. I am a life-long mixed martial arts fan. While I have never had the time or the ability to fully immurse myself into the sport, I have done my fair share of sparring and training. In 2016, I was awarded several prime territories to open Ultimate Fighting Championship (UFC) Gym franchises. My first territory was near my home in Flower Mound, Texas. My second was in the Lakewood suburb just four miles east of downtown Dallas. I had the absolute best management team at my Flower Mound location. I had challenges in Dallas during the presale and our soft-opening periods. The president of the UFC Gym Corporation and others within management referred a candidate to me. Unbeknownst to the president, I had interviewed the candidate before, and declined to present him an offer. There were certain things in his background that concerned me. Nonetheless, I was in a tight spot, and regardless of the candidate's background, he had an impressive membership sales record. Upon the president's strong recommendation, I hired the candidate at a very favorable wage. And boy, did he sell!

The candidate led the region in sales nearly every period for six weeks of his employment. He terminated historic underperformers and removed other negative influences. I could not have been more pleased with the direction of the gym . . . until I received the first bank statement. I saw that no cash had been deposited. I called him immediately. He told me the cash was in the safe, and he simply had not had the time to visit the bank. He assured me it would be taken care of that day. I trusted him at his word and went back to my busy world of forensic accounting, litigation consulting, and, of course, teaching.

A few days went by and I checked the bank account again. Nothing. I placed another call. He told me he was actually on his way to the bank just that minute. "Great." I said. "Please send me a copy of the deposit slip."

"Of course!" He quipped. I heard nothing that day and saw no deposit. It was two days away from our grand opening.

The very next day, I called to confront him. A week had now passed and I had seen nothing. As he began his excuses, I stopped him immediately, asked that he meet me at the gym, and said I would make the deposit myself. He agreed . . . and called a few moments later to resign, saying "the job was simply too stressful." Well, it was about to become much more stressful for this deadbeat.

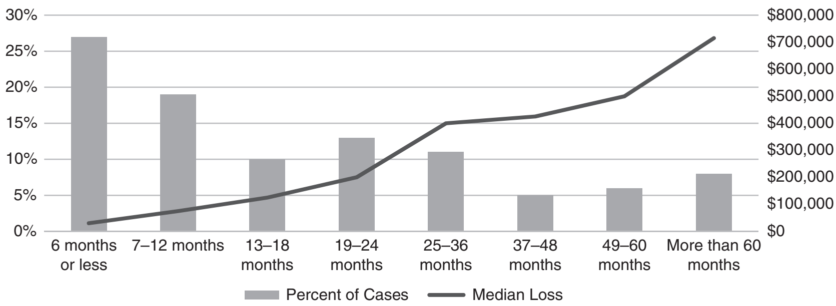

FIGURE 1.1 Duration of a fraud and median loss. *Source*: Based on data from ACFE 2018 *Report to the Nation*.

The safe was empty. No checks and no cash. We immediately began reviewing the security cameras (which are highly effective, if you are able to monitor them by the minute). We saw him regularly pocketing cash, as well as giving his girlfriend cash. I was crushed. However, considering the commissions and monetary incentive awards he forfeited, it was not a huge loss for me, and the scheme was halted after a few weeks. I turned everything over to the police, who as you can imagine were not all that enamored about pursuing my small loss. All in all, I survived, but I was embarrassed. It could have been much worse, as it generally is for so many.

While I was able to stop the fraud within a few weeks, that is not the case for most. Every two years, the Association of Certified Fraud Examiners completes a global study on occupational fraud and abuse. In their 2018 *Report to the Nation*, the ACFE found the median duration for all the fraud cases was 16 months. And obviously, as shown in Figure 1.1, the longer a fraud goes undetected, the larger the scheme will grow and the higher the loss will be.

The ACFE also examined the duration of the cases reported, based on the type of scheme involved (see Figure 1.2). Payroll schemes lasted the longest, at

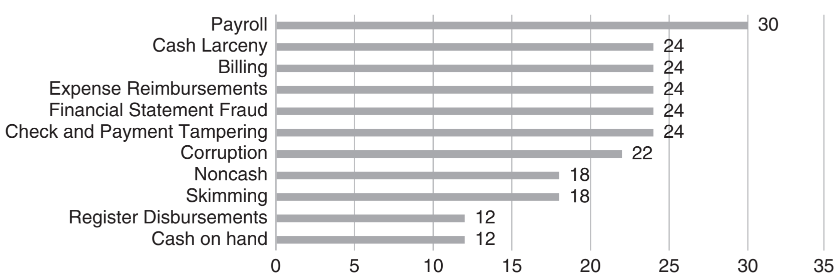

FIGURE 1.2 Duration of different occupational fraud schemes (in months). *Source*: Based on data from ACFE 2018 *Report to the Nation*.

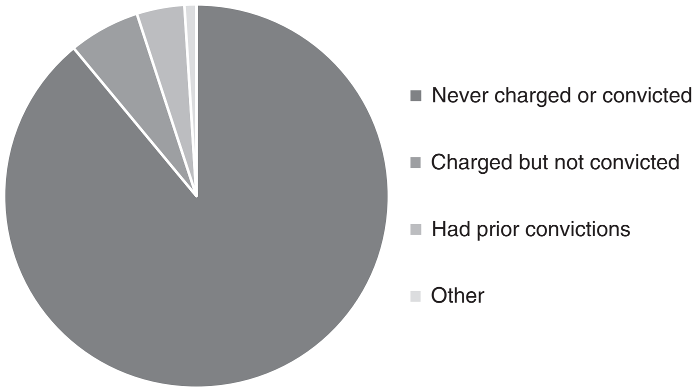

FIGURE 1.3 Percentage of perpetrators having prior fraud convictions. *Source*: Based on data from ACFE 2018 *Report to the Nation*.

30 months, whereas register disbursements, the scheme that plagued my gym, lasted six weeks. So I at least had that working for me!

And while my fraudster had prior history, another interesting fact from the 2018 *Report to the Nation* is that the vast majority of occupational fraudsters had no prior history (see Figure 1.3).

In fact, only 4% of the perpetrators in the study had previously been convicted of a fraud-related offense (see Figure 1.4). It was saddening to learn that some 40% of fraud cases are never reported to the police. However, it is understandable. Many companies fear the bad press that often accompanies a criminal or civil matter. Others simply feel it is not worth the cost or that a recovery is unlikely.

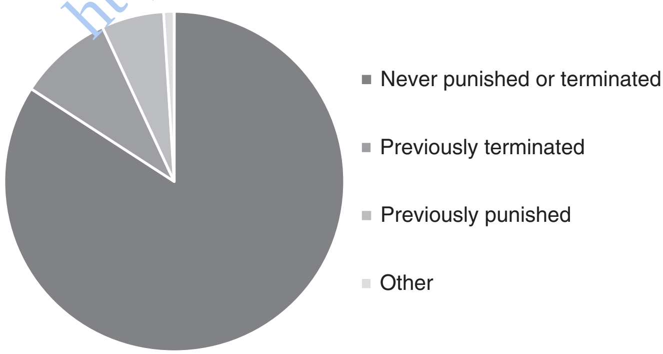

FIGURE 1.4 Percentage of perpetrators' prior employment-related disciplinary actions of fraud. *Source*: Based on data from ACFE 2018 *Report to the Nation*.

FIGURE 1.5 Comparison of fraud losses in small and large businesses. *Source*: ACFE 2018 *Report to the Nation*. © Copyright 2018 Association of Certified Fraud Examiners, Inc.

Perhaps the most provocative finding revealed in the study was the victim organizations themselves. Facts show that small organizations, those with fewer than 100 employees, experienced the greatest percentages of cases and suffered the largest median losses at $200,000, almost twice as much as the median loss larger organizations with more than 100 employees suffer. The graph in the ACFE 2018 *Report to the Nation* (see Figure 1.5) visually summarizes fraud statistics compared between small and large organizations.

I equate the disproportionate share of losses within small businesses to three common themes:

1. *Trust*. Whether the business is family-owned or a new start-up, it is entirely possible that management knows each and every employee. With that familiarity comes trust. And as we will learn, trust alone is a terrible control.
2. *Lack of resources*. Resources can consist of people and money. Small companies may find it challenging to adequately segregate critical duties, or invest in external audits (that are often not required).
3. *Lack of controls*. In addition to lacking resources, small organizations may lack the knowledge to implement adequate internal controls. It is very difficult to monitor controls that aren't there.

Additionally, I typically see more emotion when fraud is discovered at small organizations. Whereas in some cases involving fraud at large companies, perpetrators can rationalize that it is a "victimless" crime and the money wont be missed. That is not the case with small organizations. Now that you understand that fraud is happening, we will discuss your responsibilities to detect, prevent, and deter it. For the purpose of this chapter, I segregate "accountants" into three categories: (1) management, (2) external auditors, and (3) internal auditors.

MANAGEMENT

When I have been called to opine on management's responsibilities, I use guidance afforded by the Financial Executives International, or FEI. FEI is a network of 10,000+ best-in-business professionals with 65+ chapters. Founded in 1931, FEI connects senior-level executives by defining the profession, exchanging ideas about best practices, educating members and others, and working with government to improve the general economy.

FEI's mission includes significant efforts to promote ethical conduct in the practice of financial management throughout the world. Unlike Certified Public Accountants (CPAs), Certified Fraud Examiners (CFEs), and Certified Internal Auditors (CIAs), the FEI does not have a credential. They use the generic term *senior financial officers*. Nonetheless, FEI members are accountable for adhering to a Code of Ethics. The Code provides principles to which members are expected to adhere and advocate. They embody rules regarding individual and peer responsibilities, as well as responsibilities to employers, the public, and the other stakeholders. The Code reads:

All members of FEI will:

- Act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships.
- Provide constituents with information that is accurate, complete, objective, relevant, timely, and understandable.
- Comply with applicable rules and regulations of federal, state, provincial, and local governments and other appropriate private and public regulatory agencies.
- Act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing one's independent judgment to be subordinated.
- Respect the confidentiality of information acquired in the course of one's work except when authorized or otherwise legally obligated to disclose. Confidential information acquired in the course of one's work will not be used for personal advantage.
- Share knowledge and maintain skills important and relevant to constituents' needs.
- Proactively promote ethical behavior as a responsible partner among peers, in the work environment and the community.
- Achieve responsible use of and control over all assets and resources employed or entrusted.
- Report known or suspected violations of this Code in accordance with the FEI Rules of Procedure.
- Be accountable for adhering to this Code.

You will see these points echoed consistently in the pages ahead (lucky you, huh?!). Violations may result in censure, suspension, or expulsion under procedural rules adopted by the FEI's board of directors.

Perhaps the strongest component regarding senior executives' ethical dilemma toolbox are provisions set forth in the Sarbanes-Oxley Act of 2002 (SOX). On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002, which he characterized as "the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt." The general objective was to enhance corporate governance, and improve overall reliability and transparency of financial reports, and to hold those responsible for their preparation and presentation accountable for their accuracy.

One of the most significant changes as it pertains to senior financial executives was the requirements set in Sections 302 and 906.

Section 302 of the Act contains three parts: (1) accuracy and fair presentation of the report's disclosure, (2) establishment and maintenance of disclosure controls and procedures, and (3) reporting of deficiencies in, and changes to, internal accounting controls. These Civil Certifications require the CEO and CFE to personally certify the following upon filing their public reports:

1. he or she has reviewed the report;
2. based on his or her knowledge, the report does not contain any untrue statement of fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by the report; and
3. based on his or her knowledge, the financial statements, and other financial information included in the report (including, financial statements, footnotes to the financial statements, selected financial data, management's discussion and analysis of operations and financial condition and other financial information in the report), fairly present in all material respects the financial condition, results of operations and cash flows of the company as of, and for, the periods presented in the report.

A CEO and CFO must also certify that:

1. he or she and the other certifying officer:
   a. are responsible for establishing and maintaining "disclosure controls and procedures" (a newly defined term reflecting the concept of controls and other procedures of the company that are designed to ensure that information required in quarterly and annual reports is recorded, processed, summarized and reported in a timely manner) for the company;
   b. have designed such disclosure controls and procedures to ensure that material information is made known to them, particularly during the period in which the periodic report is being prepared;
   c. have evaluated the effectiveness of the company's disclosure controls and procedures within 90 days of the date of the report; and
   d. have presented in the report their conclusions about the effectiveness of the disclosure controls and procedures based on the required evaluation.
2. he or she and the other certifying officer have disclosed to the company's auditors and the audit committee (or persons fulfilling the equivalent function):
   a. all significant deficiencies in the design or operation of "internal controls" (a pre-existing term relating solely to financial reporting)

which could adversely affect the company's ability to record, process, summarize and report financial data and have identified for the company's auditors any material weaknesses in internal controls; and

b. any fraud, whether or not material, that involves management or other employees who have a significant role in the company's internal controls; and

3. he or she and the other certifying officer have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

There are a few points I would like to highlight:

1. The officer is *not* certifying that there is *no* fraud. The language clarifies that there is no fraud "based on his or her knowledge."
2. Whether the officer relies on others to oversee or address internal controls, she confirms that she, the officer, is ultimate responsible. No passing the buck!
3. Lastly, "I don't recall" is a terrible defense, as the officer confirms he has evaluated the control's effectiveness recently, i.e., within the past 90 days.

Section 906 addresses criminal penalties for certifying a misleading or fraudulent financial report. Under SOX 906, penalties can be upwards of *$5 million in fines and 20 years in prison*. Section 906 states:

1. Certification of Periodic Financial Reports. Each periodic report containing financial statements filed by an issuer with the Securities Exchange Commission pursuant to section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a) or 78o(d)) shall be accompanied by a written statement by the chief executive officer and chief financial officer (or equivalent thereof) of the issuer.
2. Content. The statement required under subsection (a) shall certify that the periodic report containing the financial statements fully complies with the requirements of section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.

There are other laws and regulations that pertain to management ethical requirements. **The Securities Act of 1933**, often referred to as the "truth in securities" law, prohibits deceit, misrepresentation, and other fraud in the sale of securities. **The Security Exchange Act of 1934,** in which Congress created the Securities and Exchange Commission, established broad enforcement authority. 17 CFR § 240.10b-5 of this Act – Employment of manipulative and deceptive devices – reads:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
>
> 1. To employ any device, scheme, or artifice to defraud,
> 2. To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
> 3. To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

In addition to the SEC's enforcement rights, private citizens also have the right to file lawsuits against companies and individuals for violations of Rule 10b-5. Typically, Rule 10b-5 claims are applied in lawsuits involving:

1. insider trading,
2. market manipulation,
3. fraud in connection with public offerings and takeovers, and
4. fraud in connection with the purchase or sale of securities.

Please understand. This is not an all-encompassing list by any stretch, and I know some amazing attorneys that can right volumes on even more rules. All industries, further segregated by country, state, and sometimes local municipalities, have their own laws, rules, and regulations. It is management's responsibility to familiarize themselves with these requirements. Therefore, consult your local regulators and attorneys for further compliance obligations.

Lastly, and perhaps most relevant, each publicly traded company is required to have an environment of oversight, that is, an operating environment in which the tone at the top encourages ethical behavior, and is the cultural element that drives the initiative. Corporate policies often include Codes of Conduct, Codes of Ethics, Fraud Policies, and annual training requirements for each.

The shortfall for many of these policies is the lack of practical examples within them, and the tendency to think that "one size fits all." Some countries have vastly different cultures and requirements. What is acceptable to some is offensive to others. Examples of common situations and cultural conflicts should be prevalent and highlighted.

Procedures and other controls include whistleblower hotlines – that is, employee reporting mechanisms, audit committees, and independent members on the company's board of directors. A common challenge is the lack of anonymity in the reporting process. Regardless of the policies and procedures implemented, there is no such thing as "guaranteed" anonymity or confidentiality.

EXTERNAL AUDITORS

Unlike management, as mentioned above, rules are defined and more restrictive when it comes to certifications and requirements of serving as an external auditor. Only Certified Public Accountants can complete a financial statement audit in the United States. The American Institute of Certified Public Accountants (AICPA) along with each state's Board of Accountants and the Public Company Accounting Oversight Board (PCAOB) promulgates CPAs rules. For the purpose of this text, I focus more heavily on the AICPA guidance. While the guidance of the two bodies is similar, it is important to note that the PCAOB monitors accountants that work with public entities, while the AICPA is more broad and is comprised of accountants ("members") that work across all areas. The AICPA bylaws require that *members* adhere to the rules of the code. Compliance with the rules depends primarily on *members'* understanding and voluntary actions, secondarily on reinforcement by peers and public opinion; and ultimately on disciplinary proceedings, when necessary, against *members* who fail to comply with the rules. *Members* must be prepared to justify departures from these rules. I have included (1) the AICPA Code of Professional Conduct and (2) SAS 99 procedures, as provided by the Auditing Standards Board of the AICPA in October 2002.

AICPA Code of Professional Conduct

AICPA is the leading professional organization for accountants in the United States. The AICPA's Code of Professional Conduct is among the AICPA's most important functions as well as a central piece of establishing and enforcing the profession's ethical and technical standards. The overarching purpose of the

AICPA Code is to ensure that its members serve the interests of their clients with a high degree of integrity, technical competency, and diligence. It has several component parts, including:

1. Members are obligated to act in the public interest. Members who act with honesty and in fulfillment of their obligation to the public to provide sound, ethical service also serve the best interests of their clients and their employers. The public consists of "clients, credit grantors, governments, employers, investors, the business and financial community, and others who rely on the objectivity and integrity of members to maintain the orderly functioning of commerce."
2. Standards of integrity. Acting with integrity means being honest and candid within the constraints of the accountant's professional obligations to maintain a client's confidentiality. Integrity also means that members must not subordinate service and the public trust to personal gain. The rules recognize that integrity can endure in the face of mistakes or differences of opinion, but vanishes when a professional acts with deceit or subordinates core ethical principles to selfish motives.
3. Standards of objectivity and independence. Objectivity is a distinguishing feature of the profession. It imposes an obligation to be impartial, intellectually honest, and free of conflicts of interest. Likewise, the Code requires accountants to be independent, precluding relationships that may appear to impair a professional's objectivity.
4. Standards of due care. Exercising due care is keeping the best interest of the client in mind as services are performed with diligence and competence.
5. Standards of scope of nature of services. In order to accomplish this, *members* should
   a. Practice in *firms* that have in place internal quality control procedures to ensure that services are competently delivered and adequately supervised.
   b. Determine, in their individual judgments, whether the scope and nature of other services provided to an audit *client* would create a conflict of interest in the performance of the audit function for that *client*.
   c. Assess, in their individual judgments, whether an activity is consistent with their role as professionals.

SAS 99

The generally accepted accounting principles (GAAP) also contain provisions to guide external auditors through their professional responsibilities as they relate to identifying fraud and misconduct. Those conducting financial statement audits are required to adhere to SAS 99. SAS 99 (also the source for

PCAOB Standard AU 316, and AU 2401, which becomes effective in 2020) not only requires auditors to be reasonably sure that financial statements are free of material misstatements, whether caused by error or fraud, but also gives them focused and clearer guidance on meeting their responsibilities to uncover fraud.

SAS 99 requires auditors to look for fraud throughout the entire audit process. The standard defines fraud as an intentional act resulting in a material misstatement in the financial statements. The standard aims to have the auditor's consideration of fraud seamlessly blended into the audit process and continually updated until the audit's completion.

SAS 99 describes a process in which the auditor (1) gathers information needed to identify risks of material misstatement due to fraud, (2) assesses these risks after taking into account an evaluation of the entity's programs and controls, and (3) responds to the results.

The auditor should also have an attitude that includes a questioning mind and a critical assessment of audit evidence (such as avoiding biases and overreliance on client representations). The engagement should be conducted recognizing the possibility of material misstatement due to fraud.

There are multiple steps involved in assessing risk of fraud (see Figure 1.6):

1. *Brainstorming*. By exercising professional skepticism, generate ideas about how and where financial statements might be susceptible to fraud.
2. *Obtaining information needed to identify risk of fraud*. Obtain information from (1) management, the audit committee, internal auditors, and others within the organization; (2) analytical procedures; (3) consideration of fraud risk factors; and (4) other sources.

FIGURE 1.6 The fraud risks assessment process.

3. *Identifying and assessing the identified risks*. Analyze information about potential fraud risks; consider the type, significance, likelihood, and pervasiveness of the risk.
4. *Responding to results of the assessment*. The risks of material misstatement due to fraud have an overall effect on how the audit is conducted. As risk increases:

   - The more experienced personnel and the greater amount of supervision are required on the engagement.
   - SAS 99 requires the auditor to consider management's selection and application of significant accounting principles as part of the overall response to the risks of material misstatement.
   - SAS 99 requires the auditor to incorporate an element of unpredictability into the procedures from year to year.

In addition, the accounts should also consult AICPA guidance in AU 240. While very similar, it provides clarity for the accountant by providing distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional. It becomes more essential to modify the nature, timing, and extent of the audit procedures the auditor will perform to address identified risks of material misstatement due to fraud, as well as performing certain tasks to address the risk of management overriding internal control and to examine adjusting journal entries, accounting estimates, and unusual significant transactions.

1. *Evaluating audit evidence*. Reminds auditors that analytical procedures conducted as substantive procedures or as part of the overall review stage of the audit also may uncover previously unrecognized risks of material misstatement due to fraud.
2. *Communicating about fraud*. Inform the proper level of management and audit committee.
3. *Documenting consideration of fraud*. Documentation is required as follows:

   - The discussion among engagement personnel in planning the audit regarding the susceptibility of the entity's financial statements to material misstatement due to fraud, including how and when the discussion occurred, the audit team members who participated, and the subjects discussed.

- The procedures performed to obtain information necessary to identify and assess the risks of material misstatement due to fraud.
- Specific risks of material misstatement due to fraud that were identified and a description of the auditor's response to those risks.
- If the auditor has not identified improper revenue recognition as a risk of material misstatement due to fraud in a particular circumstance, the reasons supporting that conclusion.
- The results of the procedures performed to further address the risk of management override of controls.
- Conditions and analytical relationships that caused the auditor to believe additional auditing procedures or other responses were required and any further responses the auditor concluded were appropriate to address such risks or other conditions.
- The nature of the communications about fraud made to management, the audit committee, and others.

The AICPA also has general standards that pertain to CPAs not conducting financial statement audits. These standards are referred to as management consulting services (MCS) standards, and accounting and review services standards. Generally, litigation services engagements are subject to the MCS standards and are exempt from the others. However, each are very similar. Consulting services that CPAs provided to their clients have evolved from advice on accounting-related matters to a wide range of services involving diverse technical disciplines, industry knowledge, and consulting skills. Most practitioners, including those who provide audit and tax services, also provide business and management-consulting services to their clients. Statements on Standards for Consulting Services are issued by the AICPA Management Consulting Services Executive Committee, the senior technical committee of the Institute designated to issue renouncements in connection with consulting services. The Council has designated the AICPA Management Consulting Services Executive Committee as a body to establish professional standards under the "Compliance with Standards Rule" of the Institute's Code of Professional Conduct (code). Members should be prepared to justify departures from this statement.

The general standards of the profession are contained in the "General Standards Rule" of the code and apply to all services performed by members. They are as follows:

a. Professional competence. Undertake only those professional services that the member or the member's firm can reasonably expect to be completed with professional competence.

b. Due professional care. Exercise due professional care in the performance of professional services.
c. Planning and supervision. Adequately plan and supervise the performance of professional services.
d. Sufficient relevant data. Obtain sufficient relevant data to afford a reasonable basis for conclusions or recommendations in relation to any professional services performed.

In "Integrity," *integrity* is described as follows: "Integrity requires a member to be, among other things, honest and candid within the constraints of client confidentiality Service and the public trust should not be subordinated to personal gain and advantage. Integrity can accommodate the inadvertent error and the honest difference of opinion; it cannot accommodate deceit or subordination of principle."

In "Objectivity and Independence," *objectivity* and *independence* are differentiated as follows: "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. *Independence* precludes relationships that may appear to *impair* a *member's* objectivity in rendering attestation services."

The "Conflict of Interest Rule" states, in part, the following:

a. A conflict of interest may occur if a *member* or the *member's firm* has a relationship with another person, entity, product, or service that, in the member's professional judgment, the client or other appropriate parties may view as impairing the *member's* objectivity. . .
b. A *member* may perform the *professional service* if he or she determines that the service can be performed with objectivity because the *threats* are not significant or can be reduced to an *acceptable level* through the application of *safeguards*. . .

Additionally, an AICPA member should also consult the following, if applicable:

1. The ethical requirements of the *member's* state CPA society and authoritative regulatory bodies such as state board(s) of accountancy
2. The Securities and Exchange Commission (SEC)
3. The Public Company Accounting Oversight Board (PCAOB)
4. The Government Accountability Office (GAO)
5. The Department of Labor (DOL)
6. Federal, state, and local taxing authorities

INTERNAL AUDITORS

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Globally, the professional is under the watchful eye of the Institute of Internal Auditors (IIA). The IIA has more than 185,000 members. The IIA in North America comprises 160 chapters serving more than 70,000 members in the United States, Canada, the Caribbean (Aruba, Bahamas, Barbados, Cayman Islands, Curacao, Jamaica, Puerto Rico, and Turks & Caicos), Bermuda, Guyana, and Trinidad & Tobago.

"Internal auditors" refers to IIA members, recipients of or candidates for IIA professional certifications, and those who perform internal audit services within the Definition of Internal Auditing.

Internal auditors serve an important function in organizations. Internal auditors can be external, meaning a company on specific assignment hires them or they can be employees to the organization. Regardless, the same standards generally apply.

The International Professional Practices Framework (IPPF) is the conceptual framework that organizes authoritative guidance promulgated by the Institute of Internal Auditors. Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Lake Mary, Florida. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security. The mission of The Institute of Internal Auditors is to provide dynamic leadership for the global profession of internal auditing.

The IIA Code of Ethics states the principles and expectations governing the behavior of individuals and organizations in the conduct of internal auditing. It describes the minimum requirements for conduct, and behavioral expectations rather than specific activities. The purpose of The Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing.

The IIA's Code of Ethics extends beyond the Definition of Internal Auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing.

2. Rules of Conduct that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

For IIA members and recipients of, or candidates for, IIA professional certifications, breaches of the Code of Ethics will be evaluated and administered according to The Institute's bylaws and administrative directives. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

Code of Ethics – Principles

Internal auditors are expected to apply and uphold the following principles:

1. Integrity: The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
2. Objectivity: Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.
3. Confidentiality: Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.
4. Competency: Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.[1]

Rules of Conduct

The IIA also has guidance of ethical conducts that includes the same principles above.

ETHICAL STANDARDS AROUND THE WORLD

To open our eyes to accounting ethical standards in other parts of the world, the following sections introduce the International Ethics Standards Board for

[1]International Standards for the Professional Practice of Internal Auditing (Standards) – IIA Standard 1210.A2.

Accountants (IESBA). The IESBA is an independent standard-setting body that serves the public interest by setting robust, internationally appropriate ethics standards, for professional accountants worldwide.[2] The IESBA is an independent standard-setting board of the International Federation of Accountants (IFAC).

IFAC is the global organization for the accountancy profession dedicated to serving the public interest by strengthening the profession and contributing to the development of strong international economies. IFAC is comprised of over 175 members and associates in more than 130 countries and jurisdictions, representing almost 3 million accountants in public practice, education, government service, industry, and commerce.[3] Members include professional organizations such as the American Institute of Public Accountants (AICPA) of the United States, the Association of Chartered Certified Accountants (ACCA) of the UK, the Chartered Accountants Australia and New Zealand, Chartered Professional Accountants Canada, Chinese Institute of Certified Public Accountants (CICPA), Institute of Chartered Accountants of India, South African Institute of Chartered Accountants, and so on. The "member bodies" of the IFAC agree to meet the standards set by IFAC-supported boards, including the IESBA.

Comparison of IESBA and AICPA Codes of Ethics

The IESBA and AICPA codes of ethics are more similar than different. Both codes address areas such as independence, due care, confidentiality, and truthful report of information. However, there are some differences between the two codes. For example, the IESBA includes three topics for professional accountants in public practice that are not specifically addressed in the AICPA Code.[4] They are:

1. Professional appointment: Ethical considerations related to the acceptance and continuance of client engagements and responsibilities of successor/predecessor accountants.
2. Second opinions: Ethical considerations related to the provision of a second opinion on the application of accounting, auditing, reporting, or other standards or principles to specific circumstances or transactions by or on behalf of a company or an entity that is not an existing client.
3. Custody of assets: Ethical considerations related to holding client assets.

[2]https://www.ethicsboard.org/.

[3]https://www.ifac.org/about-ifac.

[4]Catherine Allen, "Comparing the Ethics Codes: AICPA and IFAC," *Journal of Accountancy* 210, no. 4 (October 1, 2010).

Although they do not appear in the AICPA code of ethics, these topics are addressed specifically in the AICPA audit/attest literature and rules.

IESBA has more stringent requirements on the issue of independence than the AICPA Code. The IESBA splits its independence requirements into two sections: Section 290 and Section 291. Section 290 applies to audits and reviews of financial statements; Section 291 applies to all other assurance engagements. Section 290 has more restrictive independence requirements than Section 291 because Section 291 does not impose prohibitions or other requirements on public interest entities.

In many cases, applying either the IESBA or the AICPA Code of Ethics leads to similar results.

Updates and Recent Movements

The IESBA released a completely rewritten Code of Ethics for Professional Accountants in April 2018. The code incorporates key ethics advances and is clearer about how accountants should deal with ethics and independence issues. The new code, effective June 15, 2019, emphasizes three key messages to the professional accountants:

1. Comply with the fundamental principles;
2. Apply the conceptual framework to identify, evaluate, and address threats to compliance with the fundamental principles; and
3. Maintain independence, when required.

Next, let's take a closer look at each topic.

Fundamental Principles

A professional accountant shall comply with each of the fundamental principles. The five fundamental principles of ethics for professional accountants are:[5]

a. Integrity – to be straightforward and honest in all professional and business relationships.
b. Objectivity – not to compromise professional or business judgments because of bias, conflict of interest or undue influence of others. Objectivity is further mentioned in "Independence." Independence is defined as:
   i. Independence of mind – the state of mind that permits the expression of a conclusion without being affected by influences that

[5] *2018 Handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards),* https://www.ethicsboard.org/iesba-code.

compromise professional judgment, thereby allowing an individual to act with integrity, and exercise objectivity and professional skepticism.

   ii. Independence in appearance – the avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude that a firm's, or an audit team member's, integrity, objectivity or professional skepticism has been compromised.

c. Professional Competence and Due Care – to:
   i. Attain and maintain professional knowledge and skill at the level required to ensure that a client or employing organization receives competent professional service, based on current technical and professional standards and relevant legislation; and
   ii. Act diligently and in accordance with applicable technical and professional standards.
d. Confidentiality – to respect the confidentiality of information acquired as a result of professional and business relationships.
e. Professional Behavior – to comply with relevant laws and regulations and avoid any conduct that the professional accountant knows or should know might discredit the profession.

Do you recognize those from before? They're very similar!

The Conceptual Framework

While the fundamental principles of ethics have not changed, major revisions have been made to the unifying conceptual framework—the approach used by all professional accountants to identify, evaluate, and address threats to compliance with the fundamental principles and, where applicable, independence.

The conceptual framework specifies an approach for a professional accountant to:[6]

a. Identify threats to compliance with the fundamental principles;
b. Evaluate the threats identified; and
c. Address the threats by eliminating or reducing them to an acceptable level.

---

[6] *2018 Handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards*, https://www.ethicsboard.org/iesba-code.

New Code highlights include:[7]

a. Revised "safeguards" provisions better aligned to threats to compliance with the fundamental principles;
b. Stronger independence provisions regarding long association of personnel with audit clients;
c. New and revised sections dedicated to professional accountants in business (PAIBs) relating to:
d. Preparing and presenting information; and
e. Pressure to breach the fundamental principles.
f. Clear guidance for accountants in public practice that relevant PAIB provisions are applicable to them;
g. New guidance to emphasize the importance of understanding facts and circumstances when exercising professional judgment; and
h. New guidance to explain how compliance with the fundamental principles supports the exercise of professional skepticism in an audit or other assurance engagements.

In summary, the IESBA sets ethical principles and a conceptual framework for professional accountants to follow in more than 130 countries around the world. Many countries, such as China, put emphasis on convergence with the IESBA Code of Ethics. However, rules also vary by countries.

Ethical Standards in China

The public accounting industry is relatively new in China. The Accounting Law of 1985 was amended in 1999, and it stipulates that professional accountants must abide by ethical requirements. In June 1996, the Ministry of Finance released the Regulation of the Accounting Foundation Work, which includes ethical requirements for all accountants.

The Chinese Institute of Certified Public Accountants (CICPA) is authorized to establish professional standards and rules for CPAs. In 2009, the CICPA released the Code of Ethics for Chinese CPAs and the Code of Ethics for Non-Practicing Members of CICPA, which are aligned with the 2009 IESBA Code of Ethics for Professional Accountants. These two documents regulate the ethical conducts of CPAs and nonpracticing members.

In 2014, CICPA released Q&As related to the Code of Ethics for Chinese CPAs, consisting of over 30 specific questions in such areas as conceptual

[7]IFAC press release, dated April 9, 2018, http://www.ifac.org/news-events/2018-04/global-ethics-board-releases-revamped-code-ethics-professional-accountants.

framework, firm networks, requirements of audit and assurance services on independence, and Code of Ethics for nonpracticing members and so on. It provides detailed guidance and tips to help CPAs understand the Code of Ethics and solve ethical problems encountered in practice.

In 2017, CICPA utilized an extensive comparison chart to detail the differences between the CICPA Code of Ethics and the IESBA Code. CICPA provisions are more stringent than the IESBA Code in certain areas, for example:

1. The definition of immediate family, which is broader than the IESBA Code of Ethics to align with national Chinese legislation;
2. Key audit matter rotation which in the CICPA Code of Ethics is five years on, two years off as opposed to seven years on, two years off in IESBA Code; and
3. CICPA's Code states that an auditor cannot accept any gift.

Historically, unethical behaviors were not uncommon in China. Prevalent fraudulent activities include:

1. Accountants creating journal entries according to their bosses' direction to avoid taxes.
2. Companies keeping two sets of books to hide "private funds" for employees' benefits, gifts and kickbacks given to potential clients to gain business.
3. Bribes paid to government officials for business favors.

The current China government lists anticorruption as one of its top priorities. Although it will likely take generations to change the business environment completely, China is heading in the right direction in addressing corruption.

Ethical Standards in Canada

In Canada, the authority to set ethical requirements lies in the provincial accounting bodies of the Canadian Public Accountability Board (CPAB). The CPAB reported in 2018 that the ethical requirements of the Canadian CPA Code of Professional Conduct (CPA Code) have essentially converged with the IESBA Code of Ethics.

The Public Trust Committee (PTC) of Canada's CPA profession is currently considering the recent changes in the IESBA, such as noncompliance with laws and regulations (NOCLAR) in relation to the CPA profession's existing ethical standards. As a member of the IFAC, Canadian CPA professionals are required to meet or exceed the IESBA Code. The NOCLAR applies when accountants are providing a professional service to their clients or are carrying out their duties for their employer. It includes a clear pathway to disclosure of noncompliance with laws and regulations to appropriate authorities.

The laws and regulations against corruption appear to work wonders in Canada, which ranks as the ninth-least-corrupt nation out of 176 countries, and the least corrupt nation in the Americas, according to Transparency International's 2016 Corruption Perception Index.

Ethical Standards in India

Under the Chartered Accountants Act of 1949 (revised in 2013), the Institute of Chartered Accountants of India (ICAI) was established with the authority to regulate the accountancy profession and with powers to establish regulations as necessary to fulfill its duties.[8] The ICAI's membership is comprised of Chartered Accountants, a designation protected under the Act. The Act grants ICAI authority to (i) establish initial professional development and continuing professional development (CPD) requirements; (ii) maintain a register of its members; (iii) ensure members' adherence to laws and professional standards; and (iv) investigate and discipline members for professional misconduct.

In 2002, the ICAI developed the Peer Review Mechanism that covers all audit work conducted by its members. The Peer Review Mechanism's objectives are to ensure that Chartered Accountants who are authorized to conduct audits are complying with applicable standards set by the institute. In accordance with the Companies Act of 1956 (revised in 2013), all auditors must have a practicing certificate issued by ICAI in order to conduct statutory financial statement audits. In addition to being an IFAC founding member, ICAI is a member of the Confederation of Asian and Pacific Accountants (CAPA) and the South Asian Federation of Accountants (SAFA).

Recent cases of fraudulent financial reporting, accounting frauds, and the resulting outcry for transparency and honesty in reporting have given rise to disparate yet logical outcomes. The failure of the corporate communication structure has made the financial community realize that there is a great need for skilled professionals who can identify, expose, and prevent structural weaknesses in three key areas: poor corporate governance, flawed internal controls, and fraudulent financial statements. Forensic accounting skills are becoming increasingly relied upon within a corporate reporting system that emphasizes its accountability and responsibility to stakeholders.

[8]https://www.ifac.org/about-ifac/membership/members/institute-chartered-accountants-india.

Let's look at a recent Indian case that involves these issues. Satyam Computer Services Limited ("Satyam") was once the crown jewel of the Indian IT industry, but was brought to the ground by its founders in 2009 as a result of financial crime. Satyam's top management simply cooked the company's books by overstating its revenues, profit margins, and profits for every single quarter over a period of five years, from 2003 to 2008. Satyam's top manager stated that he overstated assets on Satyam's balance sheet by $1.47 billion, and nearly $1.04 billion in bank loans and cash that the company claimed to own was nonexistent. Satyam also under reported liabilities on its balance sheet and overstated its income nearly every quarter over the course of several years in order to meet analyst expectations.

According to the founder's own public confession, Satyam had frequently used fraudulent financial reporting practices by inflating its reported revenues by 25%, its operating margins by over 10 times, and its cash and bank balance by over $1 billion. The magnitude of this fraud makes it by far the biggest accounting scandal in India's history.[9] The Satyam reporting fraud is clearly a case of abuse of accounting, in which the accounts were adjusted upward through recording fake invoices for services not rendered, recognizing revenue on these fake receipts, falsifying bank balances and interest on fixed deposits to show these fake invoices had been converted into cash receipts and were earning interest, and so on. These types of fraudulent reporting accounting practices are both illegal and unethical.

Many experts cast partial blame for the accounting scandal on Satyam's auditor, Pricewaterhouse Coopers (PwC) India, because the fraud went undetected for so many years. In fact, the global auditing firm used Lovelock and Lewis (as their agent), who audited the Satyam's books of accounts from June 2000 until the discovery of the fraud in 2009.

The SFIO Report stated, "Statutory auditors instead of using an independent testing mechanism used Satyam's investigative tools and thereby compromised on reporting standards." PwC did not check even 1% of the invoices; neither did they pay enough attention to verification of sundry debtors, which were overstated by 23% (the SFIO report says it was overstated by almost 50%). The statutory auditors also failed in discharging their duty when it came to independently verifying cash and bank balances, both current account and fixed deposits. Hence, it was required that the PwC auditors independently check with the banks on the existence of fixed deposits, but this was not done.

---

[9]"India's Satyam Scandal: A Blessing in Disguise?" China India Institute, December 20, 2015. http://www.chinaindiainstitute.com/indias-satyam-scandal-a-blessing-in-disguise-2.

PwC audited the company for nearly nine years and did not uncover the fraud, whereas Merrill Lynch discovered the fraud as part of its due diligence in merely 10 days. Missing these red flags implied either that the auditors were grossly inept or in collusion with the company in committing the fraud. The CBI, which investigated the case, also charged the two auditors with complicity in the commission of the fraud by consciously overlooking the accounting irregularities. On April 22, 2014, The Institute of Chartered Accountants of India (ICAI) imposed a lifetime ban on four auditors involved in the Satyam CA fraud.

A point has also been raised about the unjustified increase in audit fees. The PwC received an annual fee of Rs. 37.3 million for the financial year 2007–2008, which is almost twice as much as Satyam peers (e.g., TCS, Infosys, Wipro) on average pay their auditors. This shows that the auditors were being lured by the monetary incentive to certify the cooked and manipulated financial statements. Events of such nature raised doubts about statutory auditors' discharging their duty independently. Consequently, on January 24, 2009, Andhra Pradesh CID police booked two senior partners of PwC, Mr. S. Gopalakrishna and Mr. Srinivas Talluri, on charges of fraud and criminal conspiracy. In addition, the PwC had suspended the two partners, who signed on Satyam's balance sheet and are currently in prison.

International Laws and Regulations

If I may play Captain Obvious for a minute, each country has its own laws. However, there are a few laws that transcend the borders as they relate to our fraud and misconduct responsibilities. Therefore, in addition to accounting professional Code of Ethics around the world, accountants need to understand some applicable laws and regulations that affect the profession. In this section, we compare anti-bribery laws in two counties: the Foreign Corrupt Practices Act (FCPA) of the United States and the Bribery Act of the United Kingdom, as well as touch on a few laws making the news.

US Foreign Corrupt Practices Act of 1977

The Foreign Corrupt Practices Act of 1977 ("FCPA") was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. The FCPA has two provisions:

1. Anti-bribery: The anti-bribery provisions of the FCPA prohibit the willful use of the mails or any means of instrumentality of interstate commerce

corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person.

2. Record keeping. Companies whose securities are listed in the United States to meet their accounting provisions. These accounting provisions, which were designed to operate in tandem with the anti-bribery provisions of the FCPA, require corporations covered by the provisions to (a) make and keep books and records that accurately and fairly reflect the transactions of the corporation and (b) devise and maintain an adequate system of internal accounting controls.

Many companies that are household names become involved in FCPA investigations. Often times, the costs of investigations, fines, and penalties dwarf the bribes actually paid. For example, on December 8, 2011, Wal-Mart Stores Inc., the world's largest retailer, filed its 10-K filing and disclosed its FCPA investigation:

> During fiscal 2012, the Company began conducting a voluntary internal review of its policies, procedures and internal controls pertaining to its global anti-corruption compliance program. As a result of information obtained during that review and from other sources, the Company has begun an internal investigation into whether certain matters, including permitting, licensing and inspections, were in compliance with the U.S. Foreign Corrupt Practices Act. The Company has engaged outside counsel and other advisors to assist in the review of these matters and has implemented, and is continuing to implement, appropriate remedial measures. The Company has voluntarily disclosed its internal investigation to the U.S. Department of Justice and the Securities and Exchange Commission. We cannot reasonably estimate the potential liability, if any, related to these matters. However, based on the facts currently known, we do not believe that these matters will have a material adverse effect on our business, financial condition, results of operations or cash flows.

The Walmart allegations were sensational. Walmart was accused of paying $24 million in bribes to obtain permits to obtain permission to open stores in Mexico. It was reported that an in-house attorney in Mexico initiated the allegations. The attorney launched a preliminary investigation and reported the allegations to Walmart's general counsel. It was alleged that Walmart then interviewed outside counsel to lead an investigation, yet later decided to use their in-house investigators. Those investigators determined there was a "reasonable suspicion." However, after reviewing the findings, senior executives determined there was no clear violation of law.

In November 2017, Walmart disclosed they were in discussions to settle, in which Walmart would pay $283 million:

> As previously disclosed, the Company has been cooperating with the U.S. Department of Justice and the U.S. Securities and Exchange Commission with respect to their investigations regarding possible violations of the U.S. Foreign Corrupt Practices Act and there have been ongoing discussions regarding the possible resolution of these matters with the government agencies. These discussions have progressed to a point that the Company can now reasonably estimate a probable loss and has recorded an aggregate accrual of $283 million with respect to these matters. As the discussions are continuing, there can be no assurance that the Company's efforts to reach a final resolution with the government agencies will be successful or, if they are, what the timing or terms of such resolution will be.

Further, Walmart disclosed it had incurred $877 million in pre-enforcement professional fees and compliance enhancement expenses.

This is a surprising matter, considering the strong warnings and the enforcement trends involving FCPA actions. Enforcement continues to be a top priority for the SEC and DOJ (see Figure 1.7 for DOJ and SEC enforcement actions trending by year). In 2010, the SEC's Enforcement Division created a specialized unit to further enhance its enforcement of the FCPA. The new Office of Market Intelligence is responsible for the collection, analysis, and monitoring of the hundreds of thousands of tips, complaints, and referrals that the SEC receives each year. The new office helps provide the additional structure, resources, and expertise necessary for enforcement staff to keep pace with ever-changing markets and to more comprehensively investigate cases involving complex products, markets, regulatory regimes, practices, and transactions.

In Figures 1.7 and 1.8, we analyze the trends through 2018. While we see 2010 as still the high-water mark, please notice that 2018 nearly approached the combined action levels.

2009		2010		2011		2012		2013		2014		2015		2016		2017		2018	
DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC
28	14	51	26	24	25	12	12	21	8	19	9	12	10	27	32	36	10	47	17

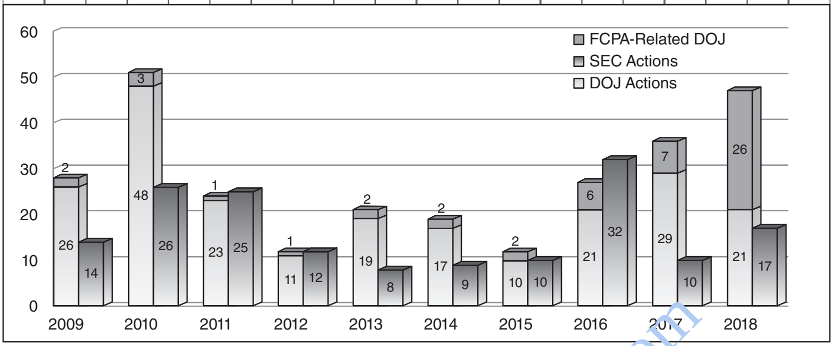

FIGURE 1.7 FCPA + FCPA-related enforcement actions (2009–2018). *Source*: Gibson Dunn & Crutcher LLP 2018 Year-End FCPA Update, 2018.

However, the most startling trend is clearly in the monetary sanctions, where as of July, the 2019 amounts are predicted to far outpace the previous high from 2009, and to continue the historical increases that began in 2016.

UK Bribery Act

A more recent bribery law is the UK Bribery Act of 2010. This Act defines offenses as offers, promises, or providing a financial or other advantage to another person, or rewarding a person for the improper performance of a function or activity. This Act also prohibits a bribe from being paid to obtain a financial or other advantage to a relevant function or for an activity to be performed improperly. The UK's Serious Fraud Office (SFO) is a specialist prosecuting authority tackling the top level of serious or complex fraud, bribery, and corruption. It is part of the UK criminal justice system covering England, Wales, and Northern Ireland, but not Scotland, the Isle of Man, or the Channel Islands.

The largest UK Bribery Act investigation involved Rolls-Royce, another household name (although I bet there are only a few of us accountants driving them!). Following a four-year investigation, the SFO reached a settlement on January 17, 2017. The DPA enables Rolls-Royce to account to a UK court for criminal conduct spanning three decades in seven jurisdictions and involving three business sectors. The settlement involves payments of £497,252,645

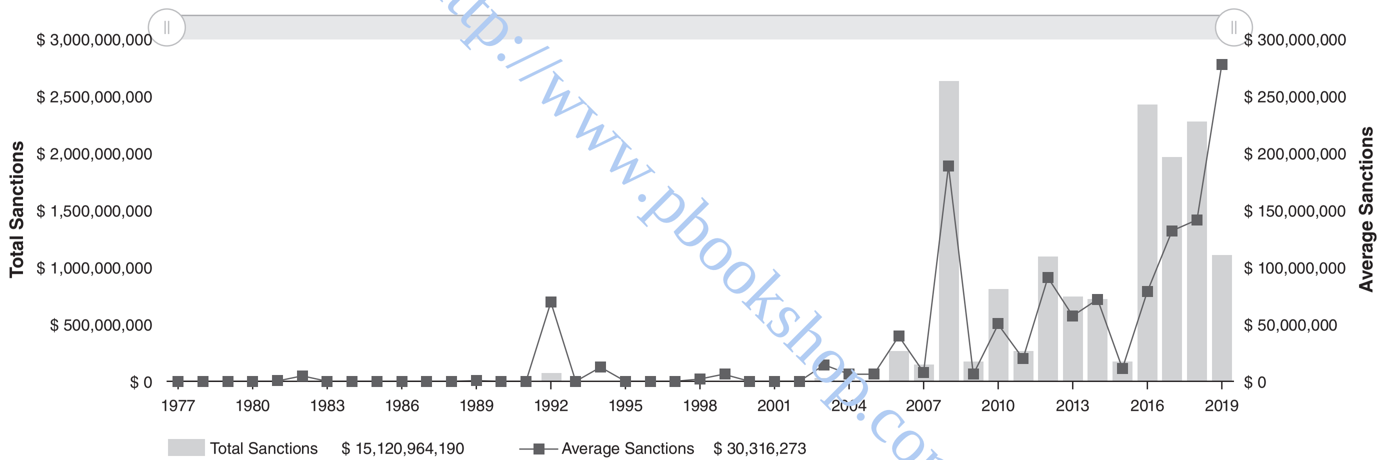

FIGURE 1.8 Total and average sanctions. *Source*: Stanford Law School in collaboration with Sullivan and Cromwell LLP.

TABLE 1.1 Differences between FCPA and the UK Bribery Act.

Element	FCPA	UK Bribery Act
Jurisdiction	Individuals affiliated with US companies, and all US companies.	Individuals who are closely connected within the UK. Companies conducting business or that are incorporated in the UK.
Enforcement	US Department of Justice (bribery provisions) and the SEC (record-keeping and internal controls).	Criminal enforcement only by the UK Serious Fraud Office (SFO).
Provisions	Record-keeping and internal control provisions.	Does not include books, records, or internal control violations.
Bribes	Prohibits bribes to foreign officials.	Prohibits bribes to foreign officials and private citizens.
Facilitation Payments	Allows payments to expedite or secure performance of a routine government action.	No facilitation payment exception.

(comprising disgorgement of profits of £258,170,000 and a financial penalty of £239,082,645) plus interest. Rolls-Royce also agreed to reimburse the SFO's costs in full (c£13m).

There are significant differences between these two Acts (see Table 1.1).

The Travel Act

While federal agencies typically use the False Claims Act (covered later), the FCPA, or the UK Bribery Act to pursue fraud, a new trend in combating healthcare fraud is the use of the Travel Act. Using this law, enacted more than 60 years ago, allows for the choosing of whether to prosecute under federal law or state law due to the alleged activity, the parties involved, and the ease of proving a violation.

The Travel Act, 18 U.S.C. § 1952, forbids the use of such transmission methods as the U.S. mail, or interstate or foreign travel, to facilitate the occurrence of criminal acts. Specially, the law states that:

> Whoever travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce, with intent to:
>
> 1. distribute the proceeds of any unlawful activity; or
> 2. commit any crime of violence to further any unlawful activity;

3. or otherwise promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity, and thereafter performs or attempts to perform
   a. shall be fined under this title, imprisoned not more than 5 years, or both; or
   b. an act described in paragraph (2) shall be fined under this title, imprisoned for not more than 20 years, or both, and if death results shall be imprisoned for any term of years or for life.

The US Department of Justice recently used the Travel Act recently to obtain multiple indictments, along with numerous guilty pleas, in healthcare investigations in Texas and New Jersey.

AUDIT VERSUS FRAUD INVESTIGATION

As we proceed through this text, it is important to understand and appreciate the difference between audit and fraud investigation. I work with both auditors and auditing professionals on a daily basis, and during my career I have assisted on more audits than I can remember. I also use auditors on my engagements as a subject matter and industry experts. That combination is a perfect complement on many of my investigations. I have also hired former auditors to work directly in my group. Some have done exceptionally well while some have struggled.

While there are many white-papers and studies that highlight the difference between a financial statement audit and a fraud investigation, the standards for each are largely the same. Both professionals are responsible for detecting fraud or errors, and there are not different levels of skepticism for each. The expectations to find fraud are likely identical to the investing public.

I have also seen narratives that attempt to differentiate the personality differences of the two. I have found those comical, and even offensive to some. In my humble opinion, only significant exposure to both professions can adequately highlight differences in the professionals. I have seen plenty of good and bad on each side, but I have also seen greatness from both.I prepared Table 1.2 based on my experiences. And while there are certainly exceptions, I find this to be an accurate representation based on my exposure.The one area that I have seen that typically determines the successful transition from an auditor to a fraud investigator is operating within the world of unknowns. Not knowing the ultimate scope, the timing, the due dates. Not having last year's working papers to refer to, and in some cases, having to completely rely on nonfinancial

TABLE 1.2 Audit versus fraud investigation.

Professional	Audit	Fraud Investigation
Certification	Auditors typically are expected to take the CPA exam and obtain a CPA license. Many public accounting firms require their staff to obtain a CPA certification before being promoted to senior associate level and beyond.	White-collar fraud investigators are oftentimes CPAs. They also commonly obtain their Certified Fraud Examiner (CFE) certification. Other certifications include Certified in Financial Forensics (CFF), and the EnCE certification, which indicates that an investigator is a skilled computer examiner. Further, many states require that investigators become licensed private investigators in the states in which they work, especially when electronic data is retrieved and used.
Backgrounds	Auditors are accountants. They can have also have valuable experience in various industries.	Investigators can have numerous backgrounds, including, but not limited to accounting, law, criminal justice, law enforcement, and the military.
Training	Technical training for CPAs focuses largely on accounting, tax, and auditing updates, as well as methodology and software tools.	Fraud examiner training centers on fraud prevention, detection, and deterrence. Depending on the investigator's practice, other specialized training focuses on financial transactions, investigation techniques, laws, and interview skills. Furthermore, research, data analysis and financial modeling are all critical areas, which are driven by the licensed technology. Training courses such as mock trials and deposition preparation are necessary for those fraud examiners who serve as expert witnesses.
Client Relationships	Financial Statement Audits are required for public registrants, governmental agencies, and many others. They are also reoccurring. The learning curve for a company's audit is steep, and costly, which makes auditor retention most common. Questions and concerns can also be	Fraud investigations are a reaction to a situation where fraud is occurring, has occurred, or is expected to occur. No one likes to see a fraud investigator, which results in "throwing good money after bad." Fraud can make executives feel cheated, angry, and hostile towards the situation. This can lead to tense environment that is best avoided. Therefore, the hope is that this is

(*Continued*)

TABLE 1.2 (*Continued*)

Professional	Audit	Fraud Investigation
	raised when a company changes auditors, so some companies are reluctant to change. As such, there is typically a long-standing, somewhat cordial relationship with a client. The relationship is carefully scrutinized to insure independence, and for publically traded companies, the audit partner must rotate every five years.	a one-time arrangement (unless outside counsel, who represents the company, hires you). There are generally no "independence" requirements for a fraud investigator.
Engagement Letter	Audit engagement letters are signed directly with the clients, the entities being audited.	Forensic service engagement letters are signed most often with in-house attorneys or outside law firms that represent the ultimate clients. This assists in preserving the confidential nature of the investigation, and attorney-client privilege.
Scope – expected work	Based on last year's working papers and well-developed, standard methodology. The number of hours per audit is generally reasonably known, and the price is often fixed.	Entirely dependent on the allegations and the investigator's experience in similar matters. It is almost impossible to know the number of hours or cost associated with an investigation. In fact, a crafty defense attorney can use fee caps and time constraints to allege that there were scope restraints.
Skepticism	Auditors assume that the client is neither honest nor dishonest. Further, each year, an auditor has to confirm they have no reason to question the integrity of management, and that there are no outstanding disagreements between them and management.	As mentioned above, an investigator is on the scene because there is belief that fraud has occured, is occurring, or is likely to occur. Therefore, there is often a mindset that someone is or is likely to be dishonest.

TABLE 1.2 (*Continued*)

Professional	Audit	Fraud Investigation
Approach	Audit covers all accounts of the financial statements. Auditors utilize sampling, statistical sampling, or nonstatistical methods. Rarely do auditors review 100% of transactions in an account, unless the account does not have many transactions. Audit utilizes threshold and materiality in testing. Transactions below a certain threshold are not selected as testing samples. Mistakes below certain materiality pass further review.	Fraud engagements are more focused, for example, on allegations involving asset misrepresentation, corruption, or fraudulent financial statements. Scope of a fraud investigation depends on the area in which fraudulent activities occurred or are suspected. Fraud investigations typically have no materiality threshold, and most likely involve reviewing 100% of the transactions in certain accounts during a period. Sometimes it is important to wear a "disguise." To avoid disrupting operations at a client, some fraud investigations are conducted covertly, or generically referred to as an audit. They are also taught to avoid using words, such as "investigation," "interview," "fraud" when meeting at client sites.
Documentation	It is imperative for auditors to have well documented work papers on all audits. Without proper documentation of work performed, an audit cannot pass various levels of reviews performed by the seniors, managers, partners, and peer review by another firm or review by higher authorities, such as PCAOB.	Fraud investigators work with sensitive information, and there are well-defined protocols that determine what, if anything, is written. Fraud investigation documentation typically would contain qualifiers such as ATTORNEY CLIENT PRIVILEGED, FOR ATTORNEYS' EYES ONLY.
Reporting	The auditor's report contains an expression of opinion on the financial statements, taken as a whole, or an assertion that an opinion	While there are many preferred templates, fraud investigation reports vary greatly in contents and format. There is no standard format or template. They can be oral or written.

(*Continued*)

TABLE 1.2 (*Continued*)

Professional	Audit	Fraud Investigation
	cannot be expressed. Audit reports have four types of opinions: unqualified opinion, qualified opinion, adverse opinion, and disclaimer of opinion.	Written reports typically contain a disclaimer to limit use of the report to certain specific purpose and audience.
	Audit reports are largely standardized to express one of four opinions.	Expert witness reports that pertain to federal matters have certain requirements in order to be accepted.
Work–life balance	Auditors typically know their schedule months in advance. The hours are long, and there are certainly "surprises" along the way, but generally speaking, their whereabouts are known.	Fraud investigators rarely know what lies ahead. When one stone is overturned, whatever is hiding underneath can sprint a number of different directions (geographies, departments, current and former executives, etc.). A $5,000 assignment can explode to a $5 million project in a split second. Assignments can also go the other direction, in that what you envision as a significant undertaking can be resolved unexpectedly through settlements and employee terminations.
	Auditors have what is referred to as "busy season," which is typically from January to the end of April. Some firms require staff auditors to work 12-hour days, along with mandatory weekends during busy season. Summers are typically a slower season for auditors, allowing them to take much deserved and needed time off.	Fraud examiners have no fixed busy season. It is feast or famine, as they jokingly put it, full of peaks and valleys. What you do in your valleys will determine how long you stay there, and also the height of your next peak. Engagements come and go at their own pace, and fraud examiners react to the demands. There are times when investigators have to work long hours for periods of time to resolve allegations. We have been known to work in 12-hour shifts, allowing coverage 24 hours per day. Further, investigations oftentimes can involve multiple countries with different time zones. Those can make for long days.

(*Continued*)

TABLE 1.2 (*Continued*)

Professional	Audit	Fraud Investigation
		Fraud examiners find it difficult to plan vacations, and certainly should insure their trips due to the sensitive and urgent nature of most matters that arise without notice.
Other interpersonal observations	I find auditors typically more organized and methodical. They are outstanding at ticking and tying financial data and supporting schedules. Their organization skills are also impeccable, and their working papers are strong. They can also be more accustomed to working in teams and "play well with others."	I find fraud investigators more skeptical, to the point of almost being cynical. (possibly a product of the environment in which they work). Their interview skills are generally more polished, and their written work-product can stand on its own.

information (interviews, surveillance, and absence of information). All of those can be overcome in time, if the professional becomes "comfortable" with being "uncomfortable."

I had the opportunity to spend time recently with a professional who has experienced all "branches" of the accounting and auditing profession during her 20-year career. She began her career as a forensic accounting consultant, and then moved into the internal audit department at an international Fortune 500 company. She then transitioned into a financial reporting role, where she interacts with the board of directors, company executives, and the external/internal auditors.

This has given her a unique perspective when it comes to responsibilities and being held accountable. I asked her the following questions:

Q: What differences come to mind, generally speaking, between a consultant and employee?

A: Employees have a vested interest in the company. They typically want to do what is in the best interest of the company and have genuine concern about their personal branding/reputation, which affects future roles, promotions, longevity with the company. Consultants are often influenced by the client and can be conflicted in doing the right thing. Consultants are also driven by sales, utilization rates, hours billed, and so on, which can often skew their intentions.

Q: While internal auditors are sometimes called "independent," what factors make that challenging? Can it impair objectivity?

A: Yes, because an internal auditor is an actual employee, and their vested interest in the company impairs their objectivity and independence. Internal auditors must balance controls, processes, and procedures with business operations so the controls do not impede productivity. Internal auditors frequently must mitigate competing priorities between a strong control environment and flourishing business operation.

Q: As a "member of management," do you now see fraud risks and ethical dilemmas differently? If yes, then how so? Would it make you a better consultant or auditor?

A: Yes, you're intimately involved in many aspects across the company, so you see fraud risks and ethical dilemmas through a different lens than a consultant, external auditor, or even internal auditor/investigator because of the closeness to the operations. You have a deeper understanding for why and how decisions were made and the justifications for them. However, you are also held to a much higher standard than an individual contributor or someone early in their career, which means despite the closeness, you can't hold any bias. As a leader of the company, you are expected to set the tone across your teams by encouraging healthy skepticism, challenging the status quo, and asking questions. You also must instill comfort in your teams so that they can report suspicions of fraud or misconduct without any repercussions.

One case that I remember fondly occurred in the early 2000s. It was a highly technical accounting matter involving one of the world's largest software developers. I was teamed with two of our firm's strongest auditors to explore various allegations involving the company's revenue recognition practices. There was an accusation that the company was recognizing revenue prematurely in violation of GAAP. The issue was whether the company's products were client-ready off the shelf – in which they could record revenue immediately – or whether the products required considerable customization, modification, and implementation – which would preclude revenue recognition.

The two auditors spent nearly 100% of their time in this particular industry on these very same issues. As such, I spent countless hours studying and compiling research. I felt ready (that I had obtained professional competency) once the assignment commenced.

We each obtained our sample of contracts for analysis. After the first few days, they had substantially completed their contract review, and I had only gone through three contracts and flagged each of them for anomalies, triggering a second level of review. Considering that I was the least experienced resource on the assignment, I took them home and studied them even closer. I compared the contracts to my research notes and even called an accounting college professor I knew. I could not get comfortable and provided my concerns to counsel.

The issue that I raised was that when I read the contract and traced the deliverables to the supporting documentation that triggered the immediate revenue recognition, I saw significant man-hours being charged to the jobs after "delivery." When I researched the employees who were incurring hours, they were classified as engineers, programmers, coders, developers, and other designers. If a product was ready "off the shelf," why did I continue to see such hours from those types of employees?

I wrote up my findings and presented them in draft form. It was the start of something far bigger than we imagined. The two auditors agreed, and went back through their contracts applying this insight, and they, too, found similar concerns. Much to the company's credit, they assisted us in the investigation, which helped reach a resolution. I can summarize management's position through the many discussions we had. They had "paralysis by analysis." There was so much data, so many reports. There were not sufficient resources or time in the day to chase down every anomaly or variance. (This is a fairly common statement across all industries.) The company ultimately was accused of overstating revenues by more than $1 billion, and settled for a $10 million civil penalty.

Was I smarter than the auditors were? Not by a long shot. I was simply accustomed to requesting and looking at documents that were often outside the scope of an audit, and for a completely different purpose. The supporting documentation was readily available, and every transaction reconciled to the data provided; there was simply more pieces to the puzzle that required a much deeper dive.

SUMMARY

Standards, standards, and more standards. And if that is not enough for you, laws, laws, and more laws. It is your individual responsibility to familiarize yourself with the standards and laws that govern your profession. These regulations constantly evolve and commonly vary by role, industry, and country. Despite the applicable standards and laws, fraud can happen to any company and any size. It is imperative that you consult the applicable rules to mitigate that risk, as well as address the occurrences as they arise.

RECOMMENDATIONS

A pervasive control, if you will, over all elements contained herein is establishing strong policies that specifically include the words *fraud* and e*thics*. In addition to using those "bad" words, those policies should:

1. Define fraud and misconduct for your organization, along with the consequences for taking part in either.
2. Be specifically tailored and communicated in a way the user will comprehend. This includes special provisions in countries that have different cultures and ethical expectations. (Language/cultural barriers do not make for good defenses.)
3. Provide illustrations, "real-world" examples that employees may face. These also include financial statement fraud and examples of management override of internal controls, specifically tailored for those involved in the accounting function. Large conglomerates should also consider the different educational backgrounds of their employees, and communicate to their level and provide examples they may commonly face.
4. Guidelines and illustrations should be certified as read *and* understood by all employees (annually); this should be accompanied by tracking mechanisms to identify those employees whose certifications are incomplete. Some companies do not stop at policies; they provide annual training, in which employees are tested based on their knowledge of the applicable policies. (CPAs and CFEs know all too well about ethical training and tests. However, not everyone is so lucky!)
5. Extended beyond employees. Agents, third-party providers, consultants, and significant vendors should also adhere to your policies and inform you when they see unethical behavior from their point of view.

6. Enforced. A strong policy is nothing more than a “paper tiger” if management fails to enforce the policy and consistently administer the consequences for breaches.
7. Constantly updates based on prior experiences.

Specially speaking to the chapter at hand, to avoid becoming a victim of F – forgetting the present, I recommend the following:

1. Keep apprised of current events. It is your personal responsibility to stay apprised of new rules and regulations affecting the profession. Regulations often alter our obligations, mostly for the better. Lawsuits, news, and other events occur weekly that involve your competitors and industry. Setting aside time each week to read and network with peers can provide valuable insight to situations that may find their way to your desk.
2. Network. As you well know, not all issues are made or become public. Attending training conferences connects you with others in your field. Further, many cities have invitation-only peer groups that confidentially share insight into emerging trends and competing priorities they face in their own environments.
3. Educate others. As you will read in the chapters ahead, you will realize that nonaccountants (or those ethically challenged accountants) can apply pressure and suggest courses of actions that violate your standards and could affect your career. Take an active approach to protecting your license and inform others of your required course of action.
4. Expect the unexpected. As you gather information through continuing education and dedication to remaining curious about the profession, document potential exposures you could face. Be prepared to encounter challenges and have a contingency plan in place if the unimaginable happens.
5. Take on a new challenge. My favorite! Be dedicated to continuous learning. Write or speak on a topic that interests you, but yet is unfamiliar. Attend a training session on an emerging area that may not currently affect you, but that could eventually. Assign something similar to those that report to you. Remain curious about the profession and encourage that in others. It is a marathon, not a sprint. And the more you learn, the more you know (my own Yogi-ism!).

Case Study: The Curious Case of the Consulting Fees

Techno Inc. is a publicly traded Fortune 500 company, with international manufacturing operations. The Vice President of Internal Audit included Techno's plant in India in this year's audit plan. During the audit's fieldwork, the team identified large payments to an Indian public official. The payments were coded as "consulting fees" in the company's general ledger. The supporting documentation was limited, as invoices contained no details, just a round dollar amounts. Techno's Indian president advised internal audit that the payments were to "ensure that operations run smoothly, and that Techno could not operate without them. It's simply the cost of doing business in India." Internal audit was told there were no contracts, no agreed-upon deliverables, and no specified pay rates or dollar figures. They also could not articulate what was actually being done.

Internal audit approached the corporate accounting department to ask why such payments were coded as "consulting fees." The Accounting Manager said he was instructed to code them as consulting payments by the CFO, who is a Certified Public Accountant. The CFO was unable to make time to meet with internal audit before their report was due to the audit committee, but through email, advised internal audit that while he had not personally reviewed the transactions or underlying support, the general counsel was aware and had asked that they be recorded this way. The CFO advised that any questions be directed toward the general counsel."

The Vice President of Internal Audit determined that in her professional opinion, these payments were bribes and likely violations of the Foreign Corrupt Practices Act. She presented her draft report to Techno's audit committee. Shortly after presenting the draft report, the Vice President was called to the General Counsel's Office. The General Counsel informed the Vice President that her assessment was wrong, and that these were truly consulting payments that he directed. He had changed her report to reflect the transaction's substance and issued the final report to the audit committee.

Further, as a result of Techno's reorganization, her role was being eliminated. However, he added, that if she signed a "nondisclosure and nondisparage agreement," she would be allowed to resign and receive six-month's severance pay including benefits. Otherwise, she would receive two weeks, with pay, and would not be eligible for rehire.

1. What "red flags" suggest these payments may not be for consulting?
2. What ethical rules, laws, or regulations are relevant to management in this situation? To internal audit? To the CFO?
3. What personal exposure exists for the accounting manager? For the CFO? For VP of Internal Audit?

(Continued)

4. What legal/financial consequences might the General Counsel be attempting to avoid by altering the internal audit report and not investigating further?
5. Alternatively, what governmental incentives suggest that the best course of action is for the General Counsel to disclose the original internal audit report?
6. What ramifications, if any, does the Vice President of Internal Audit face if she accepts the severance? And if she refuses? What pressures may influence her ultimate decision? What recourse could be available to her?
7. Assuming that Techno operates in an "at-will" state, do they face any exposure in terminating the Vice President of Internal Audit? If so, what?
8. Why might this information be of interest to the company's external auditor? What action might they take if they learned of this involuntarily?
9. Provide and defend an appropriate course of actions for each professional, including:
   a. The accounting manager in recording the transaction.
   b. The CFO, prior to acceptance.
   c. The Vice President of Internal Audit's decision.
10. If you are a Certified Fraud Examiner hired to investigation this allegation, what steps would you take to provide the company's board of directors and external auditor with the determination of their financial damages, and the opinion that this incident was isolated to India?