CONDUCTING INTERNAL INVESTIGATIONS,
U.S. EDITION



Association of Certified Fraud Examiners

GLOBAL HEADQUARTERS • THE GREGOR BUILDING
716 WEST AVE • AUSTIN, TX 78701-2727 • USA

I. PREPARING FOR AN INVESTIGATION

When Is an Investigation Necessary?

The need for an internal investigation can arise in several circumstances. Obviously, internal investigations might be necessary to determine the source of losses caused by fraud. A thorough investigation in these circumstances can enable a company to reduce its losses, identify the perpetrator, gather evidence for a criminal prosecution or civil trial, and recapture some or all of its losses. It can also identify weaknesses in the company's control structure, thereby helping to strengthen the company's internal defenses against future employee misconduct.

In addition to preventing losses due to fraud, an organization or its officers might have legal duties to investigate alleged misconduct. Certain federal statutes, such as the Foreign Corrupt Practices Act (FCPA), are specifically aimed at detecting wrongful conduct and require that companies report specific instances of misconduct. Obviously, to make an accurate report of misconduct, the management will need to investigate alleged wrongdoing. Regulatory agencies such as the Securities and Exchange Commission (SEC) require accurate financial reporting by the companies they oversee, and they have the power to impose penalties for reports that are inaccurate or omit facts that could affect the accuracy of the reported information. An investigation can ensure that all relevant facts are known and reported.

Officers and directors of companies are also bound by duties of loyalty and reasonable care in overseeing the operations of their companies. This means they must act in the best interests of the company and take reasonable steps to prevent harm that the company might suffer as a result of employee misconduct. The failure to investigate reliable allegations of misconduct can amount to a violation of this duty, thereby subjecting the director or officer to civil liability for any damages that the company incurs as a result of the failure to investigate.

In many situations, companies must also conduct an internal investigation before they can dismiss an employee who has committed fraud or otherwise violated company rules and policies. A thoroughly documented investigation will help insulate the company from charges that the employee was discriminated against or otherwise wrongfully terminated.

Where an organization might be liable for the conduct of one of its employees, an internal investigation can help mitigate the company's liability by stopping the wrongful conduct before it is allowed to grow, and by demonstrating that the company has an effective program to detect and prevent criminal misconduct by its employees—a factor that provides for the diminishment of fines under the U.S. Sentencing Guidelines (USSG) for organizations.

These are only some of the reasons that a company might choose or be compelled to conduct an internal investigation. The remainder of this section is devoted to explaining when an investigation is

called for, and how an organization can prepare itself to not only uncover the facts and evidence that are necessary to fulfill the purpose of the investigation, but also avoid the numerous legal pitfalls that await the unprepared company.

Video	
[redacted]	In the video titled "Know Your Objective," anti-fraud expert Gerry Zack, CFE, CPA, CIA, explains the importance of knowing your objective when beginning a fraud investigation. Mr. Zack is the founder and CEO of RiskTrek LLC, a consulting firm specializing in compliance, fraud, auditing, and evaluating risk. (Go to [redacted] to view the video.)

Employer's Duty to Investigate

When there are signs or suspicions of employee wrongdoing, the employer—and the fraud examiner—face two related questions: (1) whether to conduct an internal investigation of the alleged wrongdoing and (2) whether to voluntarily disclose the results of that investigation to law enforcement or other government agencies. The decision to disclose the results of an investigation is not always voluntary. In some circumstances, companies are required by law to report wrongdoing by their employees or officers. This section addresses some of the statutory and common-law duties and other factors that companies should consider in deciding whether to conduct an internal investigation. Issues relating to voluntary disclosure of the results of an internal investigation and the employer's right to keep an investigative report confidential are covered later in this workbook.

It might seem incongruous to speak of an employer's duty to investigate. After all, if an employee is stealing or otherwise behaving dishonestly, why would an employer need to be compelled to investigate? Wouldn't the company want to investigate so that it could stop the thefts, possibly recover its losses, and take steps to prevent the illegal conduct from recurring? Conducting a thorough internal investigation can result in several obvious benefits, but adverse consequences can arise as well. When a company is a victim of employee misconduct, and when that misconduct becomes public, it can potentially harm the company beyond the immediate losses from the theft itself.

As a result of public disclosure, the company might face its own criminal or civil liability or administrative fines because of an employee's misconduct for which it is legally responsible. Even if the misconduct is already public knowledge and a criminal or civil proceeding has begun, the internal investigation might have an adverse effect on the victim company. The results of the internal investigation may be subject to discovery in a civil or criminal case. Thus, by conducting an internal investigation, a company might unintentionally provide outside investigators with previously unknown evidence that could be used against the company.

EXAMPLE

Acme is under FBI criminal investigation for offenses in connection with corrupt payments to foreign officials. Acme is conducting its own internal investigation, which has focused on Larson, a clerk in the accounts payable department. Larson has refused to answer the FBI's questions, asserting his Fifth Amendment right against self-incrimination. However, Larson has responded to questions from his own company's investigators because he understands that he could be fired for refusing to comply with Acme's internal investigation. (Acme is a private employer and its employees, therefore, do not enjoy constitutional protections in connection with internal investigations.) Furthermore, Larson hopes that the internal investigation will remain confidential and that his cooperation will help him avoid more serious discipline.

However, if the FBI can obtain Larson's statements to the company or the internal report that reflects Larson's information, it would have access to information that it could not otherwise obtain from Larson due to his Fifth Amendment protections. Moreover, the government prosecutors then could contend that Larson had waived his privilege against self-incrimination by voluntarily making a statement to the company's investigator. This might enable the government to force Larson to testify. (See Chapter VI, "Legal Considerations in Interviews," for further discussion of these Fifth Amendment issues.)

Public disclosure of internal fraud can also subject a company to numerous adverse financial consequences, such as the loss of collateral business or trading partners, the loss of government licenses necessary for certain regulated activities, or a decline in the value of publicly traded equities. The directors of a corporation might face liability to their shareholders for the losses resulting from the misconduct or for any collateral consequences that result (e.g., fines or other civil liability imposed on the company). These are all factors that can incline a company toward avoiding knowledge of harmful facts.

Conversely, there are several legal duties and requirements that might outweigh a company's desire to ignore an employee or managerial offense. Many companies are required to monitor and report specific kinds of regulated transactions to various government agencies. For instance, financial institutions must file a report with the Financial Crimes Enforcement Network (FinCEN) when they suspect insider abuse by an employee. Furthermore, the officers and directors of all corporations are bound by statutory and common law standards of due care and loyalty in conducting company business.

A company's managers might find that the best way to fulfill these legal duties and requirements is to conduct an internal investigation of known or suspected misconduct. Put another way, by failing to adequately investigate, a company might not be complying with the law. Note that the decision of whether to investigate is often very fact specific, and whether an investigation is compelled by some other legal duty or requirement is best answered by the company's lawyer(s) in consultation with senior management and after a consideration of all the relevant facts.

The remainder of this section is a review of the most common legal duties and requirements that might compel or motivate a company to conduct an internal investigation.

Video



In the video titled "Continuous Monitoring," anti-fraud expert Gerry Zack, CFE, CPA, CIA, explains the importance of both fraud awareness and effective continuous monitoring. (Go to [redacted] to view the video.)

Statutory Disclosure Requirements

As mentioned earlier, several factors go into determining whether a fraud investigation should be performed. One of the deciding factors is whether an applicable law would require an inquiry into the fraud or a disclosure of known fraud to a government agency. If a law imposes such a duty and the company fails to comply, severe penalties might result. Several laws impose disclosure requirements on businesses, including:

- Monitoring and public reporting statutes
- The Sarbanes-Oxley Act
- False statement statutes
- Civil law duties to a company and its shareholders
- Accountants' and internal auditors' duties to investigate
- External auditors' duty to investigate

Monitoring and Public Reporting Statutes

There are multiple statutes and regulations that impose on companies the duty to monitor themselves, file accurate reports and statements, and keep accurate records. These laws do not explicitly require companies to conduct internal investigations; however, there might be an implied duty to investigate internal wrongdoing in order to ensure that a company meets its disclosure requirements (i.e., that its filings are accurate or that it has taken appropriate steps to self-monitor).

For example, public companies are required to file accurate financial information with the SEC. Assume that after a company files its annual report, management determines that a massive fraud might have caused a significant overstatement of the company's revenues. Since management has now learned that it filed inaccurate information, it might be required to do whatever is necessary to correct the inaccurate information. Generally, this would require the company to investigate the fraud and file corrected reports. Therefore, the company is, in effect, required to conduct an inquiry or investigation even though the law might not specifically state so.

There are several statutes and related administrative regulations that impose monitoring, recordkeeping, and reporting requirements on companies. Under these statutes, a company might have an express or implied duty to investigate internal wrongdoing.

Some statutes, such as the FCPA[1] and the Anti-Kickback Act of 1986,[2] are aimed at detecting and disclosing specific wrongful conduct (e.g., bribery of foreign officials or bribery in connection with federal contracts). Besides specifically prohibiting corrupt payments, these statutes require that companies:

- Keep accurate recordkeeping concerning subject transactions.
- Report findings of specific misconduct.
- Establish appropriate procedures to prevent and limit the offending conduct.

Other statutes, such as federal and state securities and banking statutes, do not mandate reporting of specific forms of misconduct, but instead require companies in certain regulated industries and activities to prepare and file accurate financial statements and public reports (such as prospectuses, proxy statements, and annual reports) concerning a company's affairs. These reporting requirements carry with them an implied duty to report certain forms of wrongdoing.

Companies subject to such monitoring and reporting statutes must take steps to avoid omitting or inaccurately reporting facts (including incidents of internal misconduct) that might affect a statement's accuracy. Violations of these public reporting statutes do not always require fraudulent intent or willful falsification. Furthermore, these statutes may be violated not just when management knows of reportable misconduct and fails to report it, but also when it has indications of possible wrongdoing that it does not disclose.

For example, the SEC enforces the FCPA and other federal securities laws through administrative rules such as:

- Rule 10b-5(b), which prohibits untrue statements or omissions of material facts in the sale of securities
- Rule 13b-2(1), which prohibits falsification of "books, records, and accounts" subject to federal securities laws
- Rule 13b-2(2), which prohibits an officer or director from making a materially false or misleading statement or omission to an accountant in connection with an audit or examination, or a submission to the SEC required by federal securities laws

The SEC takes the position that senior management and corporate counsel who fail to investigate alleged misconduct and fail to establish appropriate procedures for limiting the prohibited conduct may

[1] 15 U.S.C. §§ 78dd-1, 78dd-2, 78m et al.
[2] 41 U.S.C. §§ 51–58.

be held liable for violating the FCPA. Similarly, directors and others specified in reporting statutes are responsible for ensuring the accuracy of required corporate public filings, such as prospectuses, proxy statements, and annual reports. The SEC has held directors liable, among other things, for insufficient efforts to ensure that adequate information and reporting systems are in place and for ignoring weaknesses in those systems. Moreover, in the SEC's view, liability for reporting violations might exist not only when responsible individuals actually know of misconduct, but also where they know of facts that indicate possible wrongdoing. The SEC has stated that it will not tolerate "benign indifference" to employee misconduct.

Thus, an internal investigation might be appropriate or necessary under some circumstances to ensure that public statements and reports are accurate and, where required, to establish adequate procedures to prevent and limit the illegal conduct. The failure to investigate can lead a company to include inaccurate or misleading facts in public filings, for which the company and its directors and other senior management may be held liable even absent fraudulent intent or actual knowledge of the falsehoods.

Management also can incur liability if it fails to inform outside auditors of misconduct that could cause material contingent liabilities or loss of income. By failing to disclose such liabilities or losses, the organization's required financial statements might not meet generally accepted accounting principles (GAAP) and might be considered inaccurate or misleading, which is a violation of federal and state securities statutes and regulations. In those cases, using an internal investigation to discover—and report—accurate facts about the misconduct might be the most appropriate action that senior management can take to ensure that financials are accurate and in compliance with GAAP.

The Private Securities Litigation Reform Act of 1995 underscores the importance of an appropriate company response to facts that suggest employee or management misconduct. Under this Act (which is an amendment to the 1934 Securities Exchange Act), an outside accountant who learns of material illegal acts by the audited company or its employees may be required to inform the SEC if the audited company's management fails to take corrective action after it is notified of the illegal acts. Thus, in this scenario, the audited company may be required to initiate an internal investigation to determine if the allegations are true, and, if so, what actions are required to correct the situation.

Under these monitoring and disclosure statutes, a company's duty to disclose—and therefore to investigate—typically pertains to facts that are material to the financial statement or other public report. Determining what is material for purposes of these statutes can be complex and is beyond the scope of this course. Legal counsel should be consulted in such cases. However, by way of example, the SEC has found employee or management misconduct to be material in each of the following circumstances:

- The misconduct causes a contingent liability or loss of income or other adverse financial impact that must be shown in the financial statements under GAAP.

- The misconduct reflects on management's integrity.
- A significant amount of the company's business depends on the misconduct.

Sarbanes-Oxley Act

On July 30, 2002, President George W. Bush signed into law the Sarbanes-Oxley Act (SOX). This law, which was triggered in large part by several corporate accounting scandals in 2001 and 2002, significantly changed the laws of corporate governance and the rules and regulations under which accounting firms must operate. The Sarbanes-Oxley Act was designed to restore investor confidence in capital markets and help eliminate financial statement fraud in publicly traded companies, while at the same time significantly increasing the penalties for corporate accounting fraud. The most significant changes brought on by the Act include:

- The creation of the Public Company Accounting Oversight Board (PCAOB)
- Requirements for senior financial officers to certify SEC filings
- New standards for audit committee independence
- New standards for auditor independence
- Enhanced financial disclosure requirements
- New protections for corporate whistleblowers
- Enhanced penalties for financial crime

Since the enactment of Sarbanes-Oxley, the SEC has issued numerous rules and interpretations that support and expand the Act's requirements. Below is a summary of some of the most important provisions of Sarbanes-Oxley and the corresponding SEC Releases that relate to fraud detection and prevention. Because these rules are extensive and ever-changing, auditors should periodically review the SEC's website for updates and new rules at [redacted]

Public Company Accounting Oversight Board

Section 101 of the Sarbanes-Oxley Act establishes the Public Company Accounting Oversight Board (PCAOB), whose purpose is:

> *[T]o oversee the audit of public companies that are subject to the securities laws, and related matters, in order to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies the securities of which are sold to, and held by and for, public investors.*

In short, the PCAOB is charged with overseeing public company audits, setting audit standards, and investigating acts of noncompliance by auditors or audit firms. The PCAOB is appointed and overseen by the SEC, which is part of the executive branch. It is to be made up of five individuals—two who are or have been Certified Public Accountants (CPAs) and three who have never been CPAs. The PCAOB members are appointed by the SEC.

The Act lists the PCAOB's duties, which include:

- Registering public accounting firms that audit publicly traded companies
- Establishing or adopting auditing, quality control, ethics, independence, and other standards relating to audits of publicly traded companies
- Inspecting registered public accounting firms
- Investigating registered public accounting firms and their employees, conducting disciplinary hearings, and imposing sanctions when justified
- Performing such other duties as are necessary to promote high professional standards among registered accounting firms, to improve the quality of audit services offered by those firms, and to protect investors
- Enforcing compliance with the Sarbanes-Oxley Act, the rules of the PCAOB, professional standards, and securities laws relating to public company audits

REGISTRATION WITH THE BOARD

Public accounting firms must be registered with the PCAOB to legally prepare or issue an audit report on a publicly traded company. To become registered, accounting firms must disclose, among other things, the names of all public companies they audited in the preceding year; the names of all public companies they expect to audit in the current year; and the annual fees they received from each of their public audit clients for accounting, audit, and non-audit services.

AUDITING, QUALITY CONTROL, AND INDEPENDENCE STANDARDS AND RULES

Section 103 of the Act requires the PCAOB to establish standards for auditing, quality control, ethics, independence, and other issues relating to audits of publicly traded companies. Although the Act places the responsibility on the PCAOB to establish audit standards, it also sets forth the following rules that the PCAOB is required to include in those auditing standards:

- Audit work papers must be maintained for at least seven years.
- Auditing firms must include a concurring or second-partner review and approval of audit reports, as well as concurring approval in the issuance of the audit report by a qualified person other than the person in charge of the audit.
- All audit reports must describe the scope of testing of the company's internal control structure and must present the auditor's findings from the testing, including an evaluation of whether the internal control structure is acceptable and a description of material weaknesses in internal controls and any material noncompliance.

INSPECTIONS OF REGISTERED PUBLIC ACCOUNTING FIRMS

The Act also authorizes the PCAOB to conduct regular inspections of public accounting firms to assess their degree of compliance with laws, rules, and professional standards regarding audits. Inspections are to be conducted once a year for firms that regularly audit more than 100 public companies, and at least once every three years for firms that regularly audit between 100 or fewer public companies.

INVESTIGATIONS AND DISCIPLINARY PROCEEDINGS

The PCAOB has the authority to investigate registered public accounting firms (or their employees) for potential violations of the Sarbanes-Oxley Act, professional standards, any rules established by the board, or any securities laws relating to the preparation and issuance of audit reports. During an investigation, the PCAOB has the power to compel testimony and document production.

Additionally, the PCAOB has the power to issue sanctions for violations or for noncooperation with an investigation. Sanctions can include temporary or permanent suspension of a firm's registration with the board (which would mean that the firm could no longer legally audit publicly traded companies), temporary or permanent suspension of a person's right to be associated with a registered public accounting firm, prohibition from auditing public companies, and civil monetary penalties of up to $750,000 for an individual and up to $15 million for a firm.

Certification Obligations for CEOs and CFOs

One of the most significant changes affected by the Sarbanes-Oxley Act is the requirement that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) of public companies personally certify annual and quarterly SEC filings. These certifications essentially require CEOs and CFOs to take responsibility for their companies' financial statements and prevent them from delegating this responsibility to their subordinates, then claiming ignorance when fraud is uncovered in the financial statements.

There are two types of officer certifications mandated by Sarbanes-Oxley: criminal certifications, which are set forth in Section 906 of Sarbanes-Oxley, and civil certifications, which are set forth in Section 302 of the Act.

CRIMINAL CERTIFICATIONS (SOX § 906)

Under Section 906, all periodic filings with the SEC must be accompanied by a statement, signed by the CEO and CFO, which certifies that the report fully complies with the SEC's periodic reporting requirements and that the information in the report fairly presents, in all material respects, the financial condition and results of operation of the company.

These certifications are known as "criminal certifications" because the Act imposes criminal penalties on officers who violate the certification requirements.

- Corporate officers who *knowingly* violate the certification requirements are subject to fines of up to $1 million and up to 10 years' imprisonment, or both.
- Corporate officers who *willfully* violate the certification requirements are subject to fines of up to $5 million and up to 20 years' imprisonment, or both.

CIVIL CERTIFICATIONS (SOX § 302)

Section 302 of the Act requires the CEO and CFO to personally certify the following six items in every annual and quarterly report:

1. They have personally reviewed the report.
2. Based on their knowledge, the report does not contain any material misstatement that would render the financials misleading.
3. Based on their knowledge, the financial information in the report fairly presents in all material respects the financial condition, results of operations, and cash flow of the company.
4. They are responsible for designing, maintaining, and evaluating the company's internal controls; they have evaluated the controls within 90 days prior to the report; and they have presented their conclusions about the effectiveness of those controls in the report.
5. They have disclosed to the auditors and the audit committee any material weaknesses in the controls and any fraud, whether material or not, that involves management or other employees who have a significant role in the company's internal controls.
6. They have indicated in their report whether there have been significant changes in the company's internal controls since the filing of the last report.

INTERNAL CONTROLS

Under Section 404 of the Sarbanes-Oxley Act and SEC Release Nos. 33-8238 and 34-47986, management's responsibility pertaining to the company's internal control over financial reporting has been increased substantially.

DEFINING INTERNAL CONTROL

Internal control over financial reporting (ICOFR) is defined as "a process designed … to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles …."

Additionally, ICOFR is deemed to include all policies and procedures that:

- "Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the [company];
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the [company] are being made only in accordance with authorizations of management and directors of the [company]; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the [company's] assets that could have a material effect on the financial statements."

Examples of internal controls covered by Section 404 and the related Releases and Standards include, but are not limited to:

- Controls over initiating, authorizing, recording, processing, reconciling, and reporting significant account balances, transactions, and disclosures included in the financial statements
- Controls related to the prevention, identification, and detection of fraud
- Controls related to the initiating and processing of non-routine and non-systematic transactions
- Controls related to the selection and application of appropriate accounting policies

MANAGEMENT'S REPORT ON INTERNAL CONTROL

The provisions of Section 404 require management to acknowledge its responsibility for the ICOFR of the company and to assess the operating effectiveness of those controls. As a result, public companies must issue an additional internal control report within their annual report. The report on internal control should contain the following information:

- A statement of management's responsibility for establishing and maintaining adequate ICOFR
- A statement identifying the framework that management used in conducting the assessment of the effectiveness of the company's ICOFR
- Management's assessment of the effectiveness of the company's ICOFR as of the end of the company's most recent fiscal year, including disclosure of any material weaknesses identified in the company's ICOFR and an explicit statement as to whether the ICOFR is effective
- A statement that the company's independent auditor has issued an attestation report, which must also be filed with the annual report, covering management's assessment of the company's ICOFR

MANAGEMENT'S ASSESSMENT OF INTERNAL CONTROL

In performing the ICOFR assessment, management must choose a suitable internal control framework against which to evaluate the design and effectiveness of the company's ICOFR. The most commonly used model in the United States is the *Internal Control—Integrated Framework* established by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, which provides five components of effective internal controls:

- Control environment
- Control activities
- Risk assessment
- Information and communication
- Monitoring activities

Further detail on the Internal Control—Integrated Framework is available at the COSO website:



Additionally, management must carry out the following tasks:

- Determine which internal controls to test in performing the assessment, considering the significance of each control both individually and in the aggregate.
- Evaluate whether the failure of a control could result in a misstatement to the financial statements, the likelihood and magnitude of any resulting misstatement, and whether other controls are in place to mitigate this occurrence.
- Determine which locations or business units to include in the assessment, if applicable.
- Evaluate the design and operating effectiveness of the internal controls using the internal control framework chosen as a guide.
- Evaluate the probability of occurrence and the size of potential misstatements resulting from the internal control deficiencies identified and determine whether they, either individually or in the aggregate, constitute material weaknesses (any deficiency where the likelihood of potential misstatement is more than remote) or significant deficiencies (any deficiency where the likelihood of potential misstatement is more than remote and the magnitude is more than inconsequential).
- Provide sufficient documentation to support the assessment of ICOFR, including documenting the design of the internal controls and the results of management's testing and evaluation.
- Communicate the assessment findings to the independent auditor and any other applicable parties.

Recognizing that each company differs regarding internal control structure, the rules state that the nature of the testing performed by management will depend on the specific circumstances of the company and the significance of the control being tested. However, the rules also assert that inquiries alone are generally not a sufficient basis for management's assessment.

In July 2007, the SEC issued guidance specifically addressed to management about fulfilling its responsibilities pertaining to reporting on internal control over financial reporting. The guidance emphasizes a top-down, risk-based approach to management's evaluation of ICOFR and explicitly states that an evaluation performed in compliance with the guidance is one way that management can satisfy the internal control requirements established by Sarbanes-Oxley. In providing direction to assist companies' management in evaluating and assessing the ICOFR, the guidance addresses the following topics:

- Identifying financial reporting risks and controls
- Evaluating evidence of the operating effectiveness of ICOFR
- Reporting considerations

CODE OF ETHICS

As required by Section 406 of the Act and SEC Release No. 33-8177, public companies must disclose in their annual report whether they have adopted a code of ethics for senior financial officers, and if they have not, they must explain their reasoning.