PacificCPE

COURSE
11601A

Fraud Detection Fundamentals for Professionals

Fraud costs organizations billions each year, and CPAs are often on the front lines of catching it. This chapter introduces the core concepts of fraud detection, helping you recognize the warning signs, understand how fraud schemes are structured, and apply practical techniques to uncover financial misconduct. Whether you work in audit, tax, or advisory services, building a strong foundation in fraud detection makes you a more effective and valuable professional.

CREDIT HOURS 2 | FIELD OF STUDY AUDITING | EXAM QUESTIONS 10

Start Course ↓ | Final Exam Copy ↓

LEARNING ASSIGNMENTS AND OBJECTIVES

Assignment

- Study the full course materials included here.
- Complete the review questions after each chapter.
- Answer 10 final exam questions.
- Final exam is scored immediately, 70% or better passes.
- Certificate of completion is available in your account.
- Failed exams can be retaken free of charge.

Course Objectives

- Identify various types of red flags associated with financial fraud.

Copyright Notice

© 2026 Pacific CPE, LP. All rights reserved.

This course and test have been adapted from supplemental materials and uses partial text from the materials entitled Forensic Accounting and Fraud Examination, Third Edition by Mary-Jo Kranacher and Richard A. Riley, Jr. © 2024 by John Wiley & Sons, Inc. Displayed by permission of the publisher, John Wiley & Sons, Inc., Hoboken, New Jersey..

The materials in this course — including the text, illustrations, exhibits, examples, exam questions, and review questions — are the copyrighted property of Pacific CPE, LP. No portion of this course may be reproduced, stored in a retrieval system, distributed, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Pacific CPE, LP, except for the personal, non-commercial use of the registered learner.

Pacific CPE, LP grants the registered learner a single-seat, non-transferable license to access this course for the purpose of completing the associated continuing professional education credit. Account credentials may not be shared.

This course is provided "as is" for educational purposes. While Pacific CPE, LP makes a reasonable effort to ensure the content is current and accurate, the materials should not be relied upon as a substitute for professional advice. Pacific CPE, LP disclaims all liability for any error, omission, or loss arising from the use of, or reliance on, the course content.

Publication Date: September 2026

TABLE OF CONTENTS

CHAPTER 01

Fraud Detection: Red Flags And Targeted Risk Assessment 4

1.01 The Fraud Prompt—Simple And Effective 5

1.02 Module 1: Corporate Governance And Fraud 6

1.03 Module 2: Fraud Detection 21

1.04 Module 3: Targeted Fraud Risk Assessment 38

1.05 Module 4: Targeted Fraud Risk Assessment In A Digital Environment. 53

Test Your Knowledge 58

Final Exam Copy 104

Glossary 65

Index .....

Chapter 1: FRAUD DETECTION: RED FLAGS AND TARGETED RISK ASSESSMENT

Chapter Objective

After completing this chapter, you should be able to:

- Identify various types of red flags associated with financial fraud.

The Job I Wanted, But Didn't Know Existed

By Stephanie Boddie, CPA, CFE

I never set out to be an accountant, but after taking a required accounting class as part of a business degree, no one was more surprised than I to realize that I liked it. I was good at solving problems with numbers, and I sensed it was probably worth exploring. A few more accounting classes confirmed that I wanted to pursue an accounting degree.

Having landed on accounting, the next question was, what area of specialization? I don't know if it was the 8:00 am start time of class or the topic itself, but it didn't take me long to learn that taxation wasn't for me. Further, after a summer internship with one of the Big Four accounting firms, I was also less than enthusiastic about the assurance tasks associated with audit work. Simply put, the two most common paths in accounting were not a good fit for me. Now what?!

Thankfully, about the time I came to this realization, I was also taking an accounting communications course where I had to give a presentation on a "unique" field within accounting. Forensic accounting quickly caught my eye. Finally! a specialization within accounting that had potential for me, given my penchant for using accounting skills to solve puzzles! I ran with it. With a little more research, I learned about the Forensic Accounting and Fraud Examination program at West Virginia University (WVU), which was leading academic activities in this niche area of accounting. Two days after graduating college in Texas, I set foot in West Virginia for the first time to start graduate classes.

As luck would have it, during one of the classes, we heard from Forensic Accountants at the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). It didn't take long to see that they genuinely enjoyed and found meaning in their work. From what I could tell, this was the job that I had always wanted but hadn't known existed.

Within a year of completing my graduate coursework at WVU, I was hired as a Forensic Auditor within ATF's Financial Investigative Services Division (FISD) and am happy to report that almost fourteen years later, I still love what I do each day. As a forensic auditor working on criminal

investigations, no two cases are the same, but each makes a difference in the communities we serve. I've been able to work everything from arson-for-profit to international firearms trafficking cases. Forensic auditors "follow the money" to determine who funds and profits from criminal activity. On any given day, my work includes identifying persons of interest, uncovering new investigative leads, substantiating criminal charges with evidence, and/or removing profit incentives from crime.

I spend plenty of time digging into financial records to break down complex information into clear and concise summaries, but I also get to assist federal agents with interviews, search warrants, and testify to my findings. As far as accounting jobs go, I don't think there's anything more interesting or fulfilling.

THE FRAUD PROMPT—SIMPLE AND EFFECTIVE

In a paper titled, "Improving Experienced Auditors' Detection of Deception in CEO Narratives" (published in the *Journal of Accounting Research*), researchers, Mark Peecher and Jessen L. Hobson, found that experienced auditors' judgments about deception are less accurate for companies later linked to fraud, regulator investigation, or class-action litigation, unless they are first instructed to look for signs of guilt in the CEO's voice. According to a University of Illinois press release, "most people have trouble figuring out when someone is deceiving them," said Peecher, the Deloitte Professor of Accountancy and associate dean of faculty at the College of Business. "The good news here is that very experienced auditors, who are hired because they're supposed to be watchdogs for society, actually have the capacity to discern when upper management is being deceptive."

Further the article noted:

> *The researchers compiled 124 judgments from 31 very experienced auditors from multiple accounting firms. Each participant provided deception judgments for four publicly traded companies, using excerpted CEO responses to analyst questions during quarterly conference calls. Software randomly drew excerpts from a population of five fraud and five non fraud companies, with the expectation that participating auditors would spot fraud accurately 50 percent of the time by chance alone. For each company, auditors also received background information and financial statements.*
>
> *While reviewing CEO answers to analyst questions, auditors decided whether they thought the financial results being discussed were fraudulent. Peecher and Hobson found that accuracy levels for spotting fraud improved from 43 percent to 70 percent when veteran auditors were given instructions to look for signs of "negative affect" during CEO narratives from conference calls.*
>
> *If you make it easier for auditors by saying 'One of the symptoms of fraud is cognitive dissonance, so keep that in mind as you listen to this real-world recording of an earnings call with an executive and when you assess if there's deception,' that's where they're able to perform substantially better than*

chance at predicting fraud," Peecher said. "And that's encouraging and something that audit firms may want to take a look at when they try to assess fraud risk of potential and current clients.

In this chapter and the following modules, we examine various tools and techniques for fraud detection and risk assessment. Those modules, along with the learning objectives include:

- Module 1 briefly introduces the interface between corporate governance and fraud. The objective of this module is for the reader to be able to describe the elements of corporate governance and its role in antifraud efforts, particularly with regard to targeted risk assessment (TRA).
- Module 2 reviews the framework for detecting fraud and anomalous activities. The goal in this module is for readers to identify and apply fraud detection tools in case scenarios.
- Module 3 takes a close examination of targeted risk assessment. The objective is for readers to be able to apply TRA knowledge to company-specific characteristics.
- Module 4 takes a look at TRA in a digital environment. Information and transactions have become increasingly electronic. As such, it's important that TRA embrace best practices in the context of the digital world in which business operates. The goal here is for the reader to be able to apply targeted risk assessment skills in case scenarios where much of the information is captured in electronic format.

MODULE 1: CORPORATE GOVERNANCE AND FRAUD

Satyam Fraud: A Failure in Corporate Governance

In January 2009, nearly a decade after a wave of financial reporting frauds in the United States, Ramalingam Raju, the chairman of an Indian IT outsourcing company, Satyam Computer Services (SAY), with more than 50,000 employees, sent a letter to the Company's Board of Directors and the Securities & Exchange Board of India. In this letter, Raju addressed the following:

- He acknowledged his culpability in hiding information that he had inflated the amount of Satyam's cash on the balance sheet by nearly $1 billion
- Satyam incurred a liability of $253 million on funds arranged by him personally
- Satyam's September 2008 quarterly revenues were overstated by 76% and profits by 97%
- He apologized for his inability to close what began as a "marginal gap between operating profits and the one reflected in the books of accounts" but it grew to an unmanageable level.

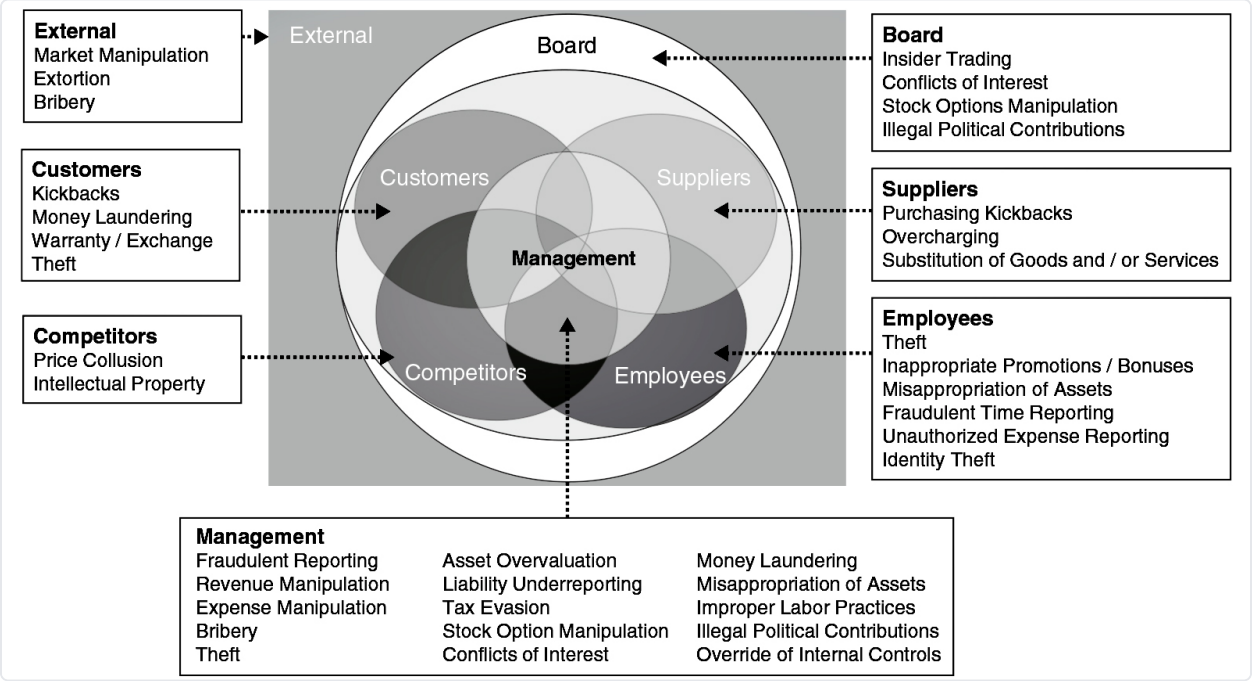
In the text of Raju's letter, he asked, "When riding a tiger, how does one get off without getting eaten?" According to SCRIBD.com, Satyam was a "failure of corporate governance." As a result, the Indian government replaced all of the Satyam Board members.

The Fraud Risk Universe

According to Jonathan Marks, CPA, CFE, CFF, in addition to establishing an ethical environment, corporate governance players, including board members and management must take the lead in establishing, implementing, and maintaining a formal fraud risk management program.

In his Blog, BoardandFraud.com, Marks identifies the fraud risk universe in Figure 1-1:

FIGURE 1-1 THE FRAUD RISK UNIVERSE



In the following section, the authors examine the critical role of the corporate governance stakeholders.

Management's Responsibility

Management's primary responsibility is to ensure that the organization meets its strategic, operational, and performance objectives. To accomplish this, the leadership must develop and implement strategies and procedures to manage the company's long-term economic stewardship rather than acting simply as agents of the owners—the shareholders—and responsible merely to maximize shareholder wealth.

Inherently, such responsibilities require that management establish some methodology for measuring performance and communicating the results of their efforts. Furthermore, management must protect the organization's assets, the various resources controlled by the organization to meets its objectives. Statement on Auditing Standards (SAS) No. 1 states, "Management is responsible for adopting sound accounting policies and for establishing and maintaining internal control that will, among other things, initiate, authorize, record, process, and report transactions (as well as events

and conditions) consistent with management's assertions embodied in the financial statements."[2] More specifically, these latter obligations require management to design and implement a system of internal controls, processes, and procedures necessary to safeguard the resources of the entity and ensure relevant and reliable financial reporting. In many cases, the company falls under the purview of various regulatory and taxing authorities that also require compliance with their informational and reporting needs.

Overall, management must design, implement, and maintain internal controls and financial reporting processes to produce timely financial and nonfinancial information that reflects the underlying economics of the business. Accounting information and reporting must comply with generally accepted accounting principles as well as other necessary regulatory requirements. Because management is responsible for the fair presentation of the financial statements and to safeguard the assets of the business, they must also mitigate fraud within the organization by preventing, deterring, and detecting asset misappropriation, corruption, and fraudulent financial statements. Consistent with those objectives, management should design, maintain, and monitor a system of internal controls over assets, financial information, and the financial reporting process. Management is also responsible for providing information to the independent auditors so that they may complete the work necessary to render an opinion on the financial statements.

The Risk of Management Override and Collusion

Depending on the individuals involved, internal controls cannot prevent management override or collusive behavior by, and among, senior management. Because prevention through segregation of duties, approvals, and authorizations is not possible in a collusive environment, the principal internal control procedures will be centered on detection. The fear of detection may serve as a deterrent, but that does not eliminate the concern that traditionally designed internal controls are ineffective when management override or collusion is present. Thus, internal and external auditors, fraud examiners, and forensic accounting professionals must design procedures to detect such activity. Because management is in a unique position to override internal controls and collude with other top managers or outside third parties, auditors and antifraud professionals must design specific procedures to determine whether the internal control system could potentially be circumvented by a senior manager through override, or by a group of managers through collusion.

Generally, three procedures are effective in identifying breakdowns in internal controls due to override and collusion.

First, journal entries recorded in the books and records, as well as other adjustments to financial information, should be examined for proper backup documentation. The auditor should obtain an understanding of the internal control processes regarding journal entries and other adjustments (such as consolidating entries that may appear only on an Excel spreadsheet) and determine whether the journal entries carry the proper authority, approvals, documentation, and sign-offs as

required by organizational policies and procedures. Further, auditors should discuss journal entries with employees who are not senior managers and inquire about inappropriate or unusual activity regarding journal entries. Often, when intentionally inappropriate journal entries are recorded, they are approved by the individual who directed and authorized it. Auditors should consider examining the timing of journal entry activity, looking for journal entries that are recorded at odd hours, such as late at night and on weekends or holidays when such journal entries may not be expected. Also, they should consider investigating journal entries that are typically used to perpetrate fraud schemes, such as reductions in liabilities and increases in revenues, or reductions in period costs and increases in capital assets, especially those made near year- end. SAS No. 99 requires testing of journal entries and other adjustments, and further details additional procedures the auditor should consider.

Second, significant accounting estimates need to be reviewed. Fraudulent financial reporting can be accomplished through manipulation of estimates that require judgment. Fabricated estimates can also be a source of concealment of other fraudulent activities. In some ways, accounting estimates may be a more effective source of fraud concealment than journal entries that involve professional judgment to determine the reasonableness of account balances. In many instances, underlying assumptions are not documented carefully or are documented with falsified or fictitious documents; these practices allow year-to-year modifications that could go unnoticed. SAS No. 99 requires auditors to consider the potential for bias when testing estimates. Included in the testing procedure should be a review of prior years' amounts to see if the methodology or underlying assumptions have changed, and if so, a determination of the business rationale for the change in approach is in order.

Third, unusual "one-time" transactions should be scrutinized to ensure that they have an appropriate underlying business rationale. Understanding the business rationale is a requirement under SAS No. 99, and is done to ensure that the financial statements are not subject to manipulation through the use of one-time, fraudulent transactions. The auditor has the responsibility to ensure that the accounting treatment is appropriate and that the transaction is properly supported, documented, and disclosed in the financial statements. Other procedures that may help to identify breakdowns in internal controls include analytical reviews in which anomalies are identified. One example is when gross margin is stable or increasing at a time when it should be decreasing, such as in a competitive environment or during an economic downturn.

As noted by Bishop et al., "many parties have pointed to the difficulty of preventing collusive fraud, as well as the large losses caused by collusion. However, relatively little is known about how collusive fraud differs from solo-offender fraud[3]." Recently, researchers have started to examine the profile of collusion and management override. First, Free and Murphy investigated co-offending and the nature of the fraud team[4]. The authors interviewed 37 convicted collusive (referred to as co-offending in research literature) fraudsters and conclude that the reasons co-offenders instigate and

commit frauds vary, based on two primary considerations: the nature of the relationship among the co-offenders and the nature of how the participants benefit from the fraud.

In contrast to interviews used by Free and Murphy and Bishop et al. conducted an analysis of the ACFE's dataset of fraud cases developed through surveys and made available to academic researchers by the Institute for Fraud Prevention.[56] This work compares solo fraud with that of collusive fraudsters and focuses on the collusive fraud leader. The authors find a number of key differences between collusive fraud and solo fraud.

- Leaders of collusive fraud tend to be younger, male, and less likely to have college degrees than solo offenders.
- Collusive fraud leaders are less likely to exhibit personal behavior issues, such as addiction problems or excessive control issues in comparison to solo offenders.
- However, collusive fraud leaders are more likely to exhibit unusually close associations with vendors or customers and to have a wheeler-dealer attitude.
- Collusive frauds are more likely to involve financial statement fraud (where arguably the organization is a significant beneficiary of the act), have larger dollar losses, and are of shorter duration. The corollary to this finding is that collusive frauds may be more difficult to conceal and maintain, causing the fraud to be revealed; it's also possible that the shorter duration is a function of the larger dollar losses being harder to conceal.
- Collusive frauds are more likely to be discovered by tip or complaint, internal audit, law enforcement, or by accident than solo fraud, highlighting the need for hotlines and other anonymous reporting mechanisms.

As stated by Bishop et al., the results highlight the importance of considering a potential fraudster's ability to build a fraud team to commit large, intense frauds[78]. The profile of the collusive team leader— younger male, close ties to customers or vendors, and wheeler-dealer attitude—contrasts with the typical notion of the white-collar criminal as older and possibly facing personal problems, such as addiction, or demonstrating control issues. Given the high cost of collusive fraud, we encourage forensic accountants, auditors, and managers to pay close attention to the profile of the collusive fraud leader and to respond accordingly when this profile is present. DiGabriele finds general agreement among academics, auditors, and forensic accountants that "forensic accounting has a place in the audit process," and the present study's findings reflect insights that should be useful to both forensic accountants and financial statement auditors as they seek to detect fraud.[9] Further, managers can consider the profile of the collusive fraud leader as they determine the deployment of antifraud resources in their organizations.

Turning to management override, SAS No. 99/113, AU 316.08 state that "Management has a unique ability to perpetrate fraud because it frequently is in a position to directly or indirectly manipulate accounting records and present fraudulent financial information ... By its nature, management