PacificCPE

COURSE

60455A

AI in Fraud Detection, Valuation, and Firm Management

Rounding out the series, this course covers the broader applications of AI across forensic accounting, fraud detection, and business valuation—then zooms out to address what it takes to manage an AI-forward firm. Topics include intelligent automation for fraud investigation, AI-assisted valuation approaches, client management strategies, project governance, and the ethical frameworks that should guide responsible AI use. Whether you're a forensic specialist, a valuation professional, or a firm leader, this course ties the full picture together with practical and forward-looking guidance.

CREDIT HOURS **2** | FIELD OF STUDY **BUSINESS** | 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

- Recall the three classifications of internal fraud as defined by the Association of Certified Fraud Examiners (ACFE).
- Recall the characteristics of financial fraud.
- Recognize the various methods used to evaluate technology.
- Recall the various parts of robots and their uses.
- Recall the characteristics of Enterprise Resource Planning (ERP) systems.
- Identify the seven steps of AI project leadership.
- Recall the potential impacts of AI on humanity.

Copyright Notice

© 2026 Pacific CPE, LP. All rights reserved.

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. Group access requires a separate enterprise license.

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.

Questions about reproduction, licensing, or use of these materials should be directed to support@pacificcpe.com.

Publication Date: May 2026

TABLE OF CONTENTS

CHAPTER 01

Intelligent Automation Of Fraud Detection 7

1.01 Detecting Fraud 7

1.02 ***Figure 12.1 The Fraud Tree*** 8

1.03 Elements Of Fraud 9

1.04 Stopscam 10

1.05 Technologies And Models 12

1.06 Our Approach 13

Test Your Knowledge 15

CHAPTER 02

Forensic Accounting 17

2.01 Forensic Accounting 17

2.02 Capability Building In Forensic Accounting 19

Test Your Knowledge 28

CHAPTER 03

Managing For Value And Valuation 30

3.01 Infinity Cycle 30

3.02 ***Figure 14.1 The Infinity Cycle*** 31

3.03 ***Figure 14.2 Value Destruction*** 32

3.04 ***Figure 14.3 Fraud In The Value Creation Cycle*** 34

3.05 Valuation 35

3.06 ***Figure 14.4 Shareholder Value Creation*** 36

Test Your Knowledge 39

CHAPTER 04

Tying It Together And Robots 41

4.01 Cycles Of Audit 41

4.02 ***Figure 15.1 The Cycles Of Audit*** 42

4.03 ***Figure 15.2 The Prmit Model*** 43

4.04 ***Table 15.2 Cash Prmit Analysis*** 46

4.05 ***Figure 15.3 Revenue Cycle Processes*** 47

4.06 Robots: A Review 48

Test Your Knowledge 52

CHAPTER 05

Client Management 54

5.01 3p Model 55

5.02 Machine Learning In Sales 59

Test Your Knowledge 61

CHAPTER 06

Ai Organization And Project Management 63

6.01 New Capability Assessment 63

6.02 Issues Of The New Organization 64

6.03 Managing Ai Projects 67

6.04 ***Figure 17.1 Ai Organizational Planning*** 67

Test Your Knowledge 70

CHAPTER 07

Governance And Ethics **72**

7.01 Some Obvious Ethical Issues 73

7.02 Governance Of Ai: An Introduction To The Problem 73

7.03 Aiai Governance Model 75

7.04 ***Figure 18.1 The*** Aiai Governance Model 76

7.05 ***Figure 18.2 The Aiai Governance Framework*** 77

7.06 Ethics Charter 77

Test Your Knowledge 79

Final Exam Copy 85

Glossary 81

Index .....

Chapter 1: INTELLIGENT AUTOMATION OF FRAUD DETECTION

Chapter Objective

After completing this chapter, you should be able to:

- Recall the three classifications of internal fraud as defined by the Association of Certified Fraud Examiners (ACFE).

We cover audit related errors and fraud throughout this course; however, this chapter is dedicated to intelligent financial fraud detection and investigation (IFFDI) using artificial intelligence (AI). The internal controls environment serves as the firewall to protect against fraud. Prevention is different than detection and detection is different than investigation. Detection implies active search to discover, find, uncover, or expose fraud. Investigation begins once a reasonable degree of suspicion develops about the likelihood that a fraud is taking place. In this chapter we will cover both detection and investigation.

When deploying your fraud detection capabilities, you will address questions such as

- How to allocate capabilities between prevention, detection, and investigation? What technologies to deploy for each?
- When and for what to use deterministic versus stochastic technologies?
- What methods, models, or techniques should you use?
- How do you design and architect your IFFDI system?
- How to protect your firm from AI-centric fraud?

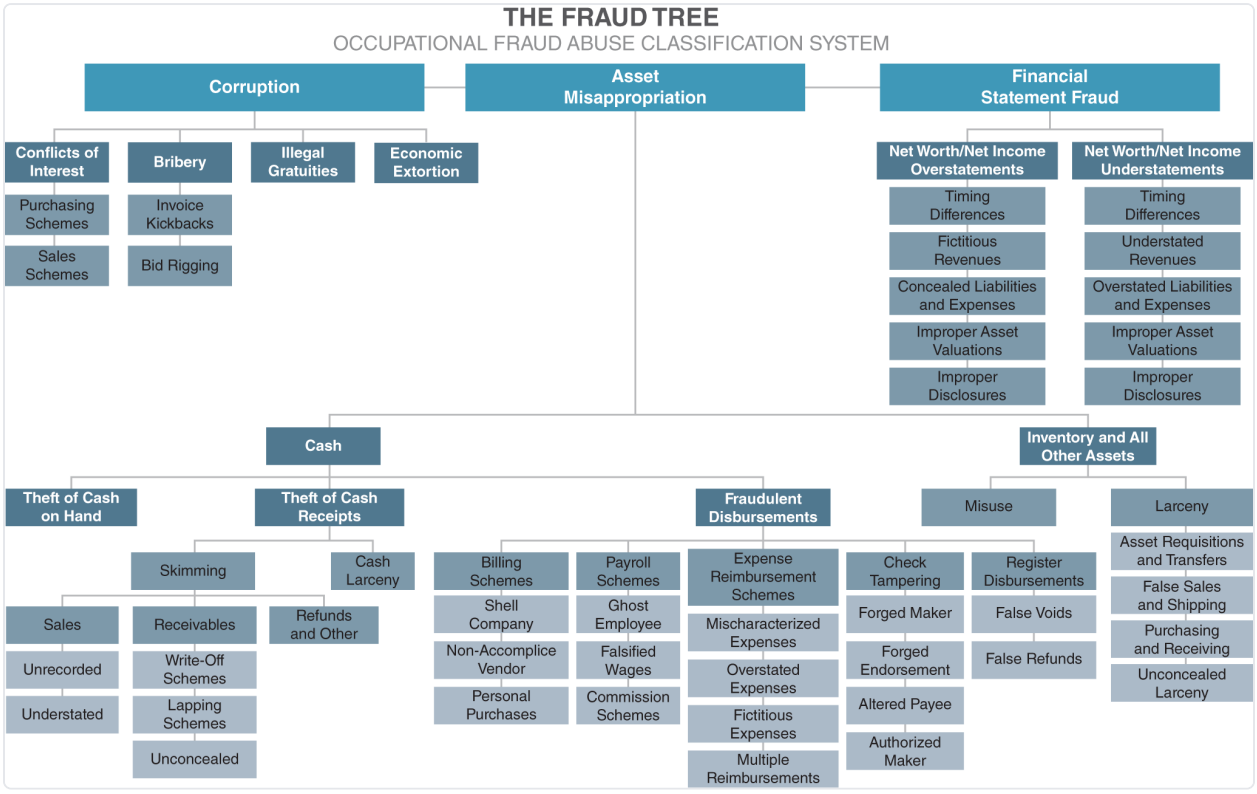
DETECTING FRAUD

Fraud happens when material misrepresentations of facts are made intentionally and they lead to loss for one or more victims. The Association of Certified Fraud Examiners (ACFE) classifies fraud against a firm into two types: internal and external (ACFE, n.d.). Internal fraud, also known as occupational fraud, is defined by ACFE as “the use of one’s occupation for personal enrichment through the deliberate misuse or misappropriation of the employing organization’s resources or assets.” Internal fraud is committed by the managers, employees, owners, or board members of a firm.

External fraud, in contrast, is conducted by parties external to the firm, for example, customers, suppliers, partners.

ACFE classifies internal fraud into three areas: corruption, asset misappropriation, and financial statement fraud. ACFE has developed a powerful and comprehensive representation of internal fraud. Known as the Fraud Tree (Figure 12.1), it covers the various subcategories and subclasses of internal fraud.

FIGURE 12.1 THE FRAUD TREE



Fraud can happen at any point in an organization. For example, it can happen at the employee level, at the board level, or across the value chain via collaboration between partners and even competitors. Detecting fraud is one of the most complex undertakings. Protecting a firm from any possible fraud can be expensive and therefore costs of IFFDI need to be considered.

Let’s not forget that in many cases savvy managers operate on the borderline of law and while technically statements and disclosures may not qualify as misrepresentations from a legal perspective, the underlying motivation for business decisions could be self-serving. For instance, the management team of a nonprofit deploys a CEO friendly board and with the board approval starts making investments

in a manner that the CEO intends to personally benefit from in the future. Such situations make fraud detection extremely hard.

ELEMENTS OF FRAUD

In the 1950s, Donald Cressey presented the fraud triangle theory that identified the three fraud elements as pressure, opportunity, and rationalization (Cressey, 1953). A fourth element of capability was later added and the model transformed from a triangle to a diamond (Wolfe and Hermanson, 2004; Mansor, 2015). As we think about intelligent automation, our design elements must first begin by analyzing the elements of fraud and building capabilities around them.

Pressure or Motivation

Preemptive detection of motivation can go a long way to detect and prevent fraud. Motivation can be anything from personal to business situations. At an individual level it could be when a person is facing financial difficulties and hence decides to engage in a fraud. On a management team level, it could be pressure to report certain earnings numbers for which guidance has been provided. Motivation determination technologies are deployed to evaluate the situations that can motivate a person or management team to commit a fraud. They typically involve understanding the situational dynamics to predict the likelihood of fraud.

Opportunity

The opportunity for fraud is based upon the internal controls weaknesses. An environment that lacks controls or that has a culture that promotes recklessness can be a fertile ground for fraud. The opportunities are identified and exploited by individuals and management teams. Fraud opportunity assessment technology is deployed to assess the control weaknesses as well as cultural and behavioral modeling to assess the seriousness and desire of the management team and boards to deploy internal controls.

Rationalization

Rationalization is the justification that a person or team gives to the conduct of fraud. This is a self-deceiving factor where teams and individuals say to themselves that it is okay to engage in a fraudulent behavior for such-and-such reasons. The justification could be that it is a one-time thing or that they are only borrowing money or that they were denied proper compensation and therefore it is their right to steal. Rationalization detection technology is composed of systems deployed to perform behavioral analysis of individuals and teams.

Capability

Capability is when a person or team believes that they have the capability to get away with doing the fraud, to not get caught, and to pull it off. Capability detection technology is also used to assess the materiality of the impact a person, machine, or team can have.

AI has been used to combat fraud by building capabilities in accordance with the fraud triangle in practice. For instance, Lin et al. (2015) employed Logistic Regression, Decision Trees, Classification and Regression Trees (CART), and Artificial Neural Networks (ANNs) to study the three aspects of the fraud triangle.

DOMAIN-SPECIFIC FRAUD DETECTION

The FBI classifies financial frauds into various areas such as securities fraud, credit card fraud, financial statement fraud, insurance fraud, and corporate other fraud. One way to approach your design is to consider each specific domain area in which you have material exposure. This means that specialized solutions need to be developed in those specific domains. Significant research exists in the use of intelligent automation for domain-specific fraud detection (Ngai et al., 2011; West and Bhattacharya, 2016).

STOPSCAM

The American Institute of Artificial Intelligence has developed a model known as STOPSCAM. This model expands upon the domain-specific model and fraud elements to develop broad classification of fraud by capability areas or detectors that focus on building and deploying intelligent capabilities. STOPSCAM is an acronym for Strategy, Transactions, Operations, Processes, Statements, Culture, Attitudes, and Model.

Strategy

The strategy tool analyzes a company’s strategy to obtain key insights to capture signals of significant changes or persistence in a company’s strategy. A sudden or abrupt change in strategy, a reluctance to change strategy when it is evident that the strategy is not working, rise of a new competitor, a change in technology, bankruptcy risk, and other strategy concepts are captured and analyzed. Strategy changes also include mergers and acquisitions and major financing events. Automated strategy analysis is performed from analyzing analyst reports, company press releases, and other news and opinions about a firm.

Transactions