PacificCPE

COURSE
11604A

Technology Tools for Fraud Examination and Forensics

Data analytics and digital tools have transformed how fraud is detected and investigated. This chapter explores how to leverage information technology in fraud examinations and financial forensics, including techniques for analyzing large datasets, identifying anomalies, and preserving digital evidence. Whether you are new to forensic technology or looking to sharpen your existing skills, this chapter provides practical guidance on integrating modern tools into your investigative workflow and strengthening the quality of your findings.

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

- Recognize the tools available to fraud examiners and forensic accountants.

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

Using Information Technology For Fraud Examination And Financial Forensics 4

1.01 Module 1: The Digital Environment 7

1.02 Module 2: Digital Evidence 10

1.03 Module 3: Detection And Examination In A Digital Environment 17

1.04 Module 5: Case Management Software 44

Test Your Knowledge 45

1.06 Data Collection Checklist 48

1.07 Comprehensive Guidelines: Information Collected In Interviews 53

Final Exam Copy 102

Glossary 63

Index .....

Chapter 1: USING INFORMATION TECHNOLOGY FOR FRAUD EXAMINATION AND FINANCIAL FORENSICS

Chapter Objective

After completing this chapter, you should be able to:

- Recognize the tools available to fraud examiners and forensic accountants.

IT Technology, Fraud Examination, and Financial Forensics Perspectives

by Mark Nigrini

In the late 1990s data analysis techniques were known as Computer Assisted Audit Tools and Techniques (CAATs). These tools were usually the specialty of one or two people in an internal audit department or in an audit office. The term big data was unheard of because the techniques were done on a desktop computer using a 486, or a Pentium chip. The analysis might have been done in Excel 97 or Excel 2000 with row limits of either 16,384 records or 65,536 records. But just because Excel could handle 16,384 or 65,536 records did not mean that your 486 or Pentium computer could process such a large file. This caused auditors to need various workarounds such as the one described in my 2012 book on Benford's Law, ". . . because of computer processing limitations the data set was too large to be analyzed in its entirety. To overcome the size issue, the internal auditors deleted all claims below $1,500. They chose this amount because they were reasonably sure that all the fraudulent claims exceeded this number."

Excel was a known commodity and it worked well in many respects, but in certain aspects it was lacking. To the rescue came specialized audit software such as IDEA (see https://idea.caseware.com/ products/idea). These specialized apps offered some advantages over spreadsheets. First, they could read and import data from many platforms and systems. Second, they kept a log of the commands used during a session and this was seen to be useful for audit working papers and to rerun those same tests at a later date on updated data. Third, users could not in any way alter the source data. What you imported was what you analyzed. If it turned out that negative net payroll payments were errors, then the user had to extract only the positive payroll payments to a new table and analyze that table going forward. Fourth, they could import and analyze, at least in theory, files with more records than the Excel maximums. The file size was still limited by the desktop's processing power.

The analytics of the late 1990s essentially fell into five camps. First came rules-based compliance auditing. For example, if Grade 3 insurance adjusters could only authorize claims up to $5,000

then an internal auditing test would verify that the limit was never exceeded. If a utility company was required to return customer deposits within 30 days of their terminating the service, then an internal auditing test would verify that the 30-day rule was followed. Second came rules-based fraud detection and forensic accounting to identify and detect ghost employees, collusive bidding, and conflicts of interest (vendors with the same address as that of an employee). Third came reasonableness tests performed on client-supplied reports. Auditors were advised that "by understanding the nature of printed reports, and then learning some testing advantages afforded by audit software (such as recalculations), that they could then place more reliance on client-supplied information." Fourth came statistical sampling where auditors applied an audit procedure to a sample (an account balance or a class of transactions) and then evaluated the results such as calculating a projection of the total misstatement. The final camp consisted of internal auditors and specialist accounts payable auditors identifying duplicate payments made by accounts payable personnel.

Fast forward to now and employers are expecting data analytics skills to be pervasive, and no longer just the talents of a chosen few. Employers are expecting accounting recruits to be technologically savvy with acronyms such as ETL as pervasive as DR, CR, and COGS, and terms such as dashboards as pervasive as double-entry. Statements such as "Employers are looking for people that are able to think analytically and are capable of approaching a problem in a structured and methodical way" are now the norm. There are no longer limits on the size of data sets that can be evaluated, because now there are specialty apps (such as R) designed to clean, organize, analyze, and visualize big data. Data is also no longer only in tables with fields and records, in that a whole new paradigm has emerged in the form of unstructured data and applications such as textual and sentiment analysis. Output is no longer also confined to reports on green bar computer paper but includes results shown in link charts and flow diagrams. Indeed, data visualization has emerged as a stand-alone skill aided greatly by the tens, if not hundreds, of options available in Tableau. Case management software has replaced documents, images, and tables, in a single "directory" named after the client and the year. Data analysis (now called audit data analytics and forensic analytics) is not limited by the power of a desktop's computer chip and the capacity of a CD but is only limited by the imagination and creativity of today's forensic accounting, financial accounting, and auditing professionals.

Mark J Nigrini, Ph.D., West Virginia University is the author of *Forensic Analytics and Benford's Law*.

How Will Artificial Intelligence Impact Accounting?

According to a 2016 article by Oliver Griffin, artificial intelligence (AI) is no longer the stuff of science fiction and Hollywood movies[1]. Griffin observes that works of film and fiction are often

hooked on the rise of artificial intelligence (AI) and such tales are often apocalyptic—*Blade Runner*, *Alien*, *Terminator*—where mankind comes off badly.

Contrary to popular fiction, the author notes that in the "real world" AI is being spearheaded by Internet giants including Google, Microsoft, and Amazon, and our daily lives are increasingly affected by seemingly intelligent systems—Siri and Alexa, purchase predictions, news generation, etc.

What does this mean for accountants? By some predictions, bookkeepers have a 97.6% chance of losing their jobs as machines take over the number crunching and data analysis[2].

According to Griffin's article, Richard Anning, ICAEW's IT Faculty, asks, "Will AI reduce the need for accountants? I think the answer is probably yes," he says. "But you have to define what an accountant is. If you're looking at some of the more repetitive bookkeeping or process-driven tasks, those are more likely to be subject to automation than the higher value tasks." As such, a younger accountant entering the profession needs to understand the AI trend and develop skills to permit working with intelligent systems.

Of no surprise, Griffin finds that AI is already beginning to automate tedious tasks such as data entry. Automation is occurring at the staff level, and automation is likely to begin to automate higher level accounting jobs.

Griffin queried Shamus Rae, a partner at KPMG, who stated, "AI will increase our audit quality, as it begins to allow us to ask a lot more questions. It will improve efficiency in what we do and it will provide more insight. More than whole jobs disappearing, we will more likely see an impact on skill sets and we will still need humanities. We want this to lead to a more holistic education for all."

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

- Module 1 introduces digital concepts associated with forensic accounting and fraud examination to the reader. The information covered here seeks to reconcile traditional "paper and pencil" techniques with the subtleties and nuances of collecting and analyzing evidence electronically. The objective of this module is for the reader to be able to identify opportunities within the digital environment for increased efficiency and effectiveness.
- Module 2 drills down into digital evidence, including sources of evidence and the need to properly collect and protect electronic evidence in a manner admissible to courts of law. The goal of this module is for readers to apply the tools and techniques associated with digital evidence to case scenarios.

- Module 3 explores the methodologies for detection and examination in a digital environment. This module includes analytical tools and techniques available in most software programs, as well as specific electronic tools, such as Excel and IDEA. The objective is for the reader to be able to identify appropriate digital approaches and use those approaches to examine digital data.
- Module 4 outlines graphical tools and techniques. Graphics serve at least three important roles for forensic and antifraud professionals: as an investigative tool, as an identifier of needed procedures, and as a communications tool. The goal here is for the reader to be able to apply graphics skills and software to case scenarios.
- Module 5 considers the tools and techniques for case management. The goal in this module is for the reader to identify when and how to use case management software.

MODULE 1: THE DIGITAL ENVIRONMENT

The purpose of this chapter is to provide an overview of the information systems control environment, as well as big data, data extraction, and analysis tools and techniques. Technology is a specialized area, and, as a result, the auditor, fraud examiner, or forensic accountant may need to solicit the assistance of a professional with expertise in digital environments, tools, and techniques. Of course, determining the required level of expertise is similar to other tasks that arise in many areas of the fraud examination or forensic accounting engagement—it requires judgment on the part of the professional involved.

The starting point for the use of electronic data in the fraud or forensic accounting area, as a means of fraud prevention and deterrence, is an evaluation of the integrity of the data and their related systems. Many have heard the acronym GIGO, "garbage-in, garbage-out." If the data going into the information system lack integrity—the data has been manipulated or corrupted, or the information processes somehow destroy the integrity of the data—any information subsequently extracted will lack integrity. Similar to the chain of custody concepts, good audit trails that allow the data to be tracked through the system are also crucial to the goal of maintaining data integrity and, just as important, the ability to prove the origins and credibility of the data.

Overview of Information Technology Controls

Many of the process controls applicable to paper-based information systems are analogous to the internal controls surrounding digital information systems. An information technology (IT) audit consists of (1) planning, (2) tests of controls, and (3) substantive tests. Further, the IT audit requires an understanding of the control environment related to IT; risk assessment of the things that could go wrong in an IT environment; and information, communications, monitoring, and independent checks of the IT systems' internal controls. Some of the control activities in an IT environment that parallel those in the world of paper include proper authorization and access controls, segregation of IT duties, IT supervision and approval, adequate record keeping, and independent supervision and

verification. More specific to IT, the general framework for viewing IT risks and controls include the following:[3]

- IT Operations
- Data Management Systems
- New Systems (Software) Development and Integration
- Systems Maintenance
- Systems Backup and Contingency Planning
- Electronic Commerce
- Control over Computer Operations (Hardware, Software, and User Access)

Each of these areas has particular control issues and needs to be examined carefully because data integrity issues can arise in any area.

Big data, data analytics, and CAATTs (computer-aided audit tools and techniques) can assist with the testing of the IT systems control environment. One of the necessary areas of concern is applications controls. Applications are systems or subsystems in the areas of accounting, finance, marketing, sales, warehousing, distribution, payroll, personnel, etc. Application controls are designed to address risks that threaten the processing and storage of data in these areas.

The first application control applies to the initial input of data. A transaction must start somewhere, and someone must have the authority to initiate that transaction. The important financial and operational attributes of that transaction must then be captured by the digital system. In paper-based systems, this is accomplished by first "writing" the transaction on paper, such as preparing an invoice, or the transaction can be entered directly into the computer system. In some cases, such as e-commerce, transactions are entered directly into the computer by participants to the transactions who are not employees of the company, ordering a product on Amazon.com is an example. In such cases, little or no traditional source documents exist in paper form. In other cases, a paper trail is created.

Similar to paper-based information systems, the source documentation that supports the electronic data systems should be logged, date and time stamped, prenumbered, and used in sequence. Supporting source documents should be audited periodically and should be retained physically, or in electronic format, because they may include transaction information; sign-offs for those who prepared the document/transaction; required approvals and other authorizations; and the identity of the person who processed the information into and/or through the application system.

Once documents or transactions are captured by the application systems, data coding controls can be used to identify transcription and transposition errors. In some cases, check digits may accompany transactions as a means of authenticating those transactions as they move throughout the system.

Batch controls are used when groups of documents or transactions are entered or processed in batches (e.g., totals for a day). Batch controls may consist of a document count or a manual sum of all the transactions to be entered, which is later compared to the electronic batch total from the computer system after entry. Batch total controls use system-generated criteria that ensure data integrity for groups of transactions as they move through the system.

Validation controls detect input errors by flagging those transactions that fall outside accepted ranges. These controls may look for numeric, alphabetical, or alpha-numeric data in a particular field, as an example. They attempt to identify and isolate errors during data input, so that the error can be addressed before those data are further processed. Validation controls can also be established to ensure that the correct file is accessed.

Record validation is another technique that ensures that data relationships within a record make sense. It can include reasonableness checks, sequence checks, and other checks. An important application control is input error correction. This control requires that all errors are properly addressed prior to the data being processed through the system.

Finally, the application input system needs to be examined, as a whole, to ensure that input errors can be identified and addressed as quickly as possible.

Once the transaction data are "inside" the application system(s), they are available for further processing and transfer to other application systems. Processing controls are necessary to ensure that processed data maintain integrity as they move through the system. These include run-to-run controls that monitor various batch totals, recalculate control totals, transaction codes, and sequence checks, as data move from procedure to procedure. Some data processing requires systems operator intervention to initiate further action. Operator intervention increases the chance of human error, so controls need to be in place to minimize this. As data are processed through the system, an audit trail also needs to be developed. The data audit trail usually includes transaction logs, logs of automated transactions, a listing of automated transactions, unique transaction identifiers, and error logs.

Once the data have been sufficiently processed, they are available for output in the form of reports, as well as for transfer to other systems for additional processing. Output controls are established for spooling (how outputs move through the system and address output backlogs), print programs, and bursting (separating and collating printed pages). Output controls also address how to monitor waste and how to identify who is responsible for data accuracy and maintenance, report distribution, and end-user controls.

IT Audits and Assurance Activities

Auditors and forensic accountants who specialize in IT audit and assurance can approach IT system controls testing by one of two major approaches. First, the IT systems can be audited around. This is

often referred to as the "black-box" approach, by which the professional relies on interviews and flowcharts to develop an understanding of the systems but primarily tests the integrity of the data and the system by reconciling inputs to outputs. The second alternative is the "white-box" approach, which utilizes a relatively small dataset to test the system. Some of the tests performed include authenticity, accuracy, completeness, redundancy, access audit trail, and rounding error tests. CAATTs can facilitate the white-box approach by creating test data and performing electronic system walk-throughs (tracing). Computer forensic professionals may employ integrated test facilities by which the auditor examines the applications and their logic during normal operations by running parallel simulations.

These examinations are necessary to ensure that the data used by the auditor or forensic accountant have integrity. Various levels of assurance are necessary, depending on the engagement. Professionals in this environment need to be cognizant of the possibility that one or more of the IT systems personnel may be colluding with others to commit or conceal fraud. As such, fraud and forensic accounting professionals need to remain alert to the human side of fraud, the fraud triangle (pressure, opportunity, and rationalization), as well as M-I-C-E (motivations such as money, ideology, coercion, and ego). In fact, the IT professional may be in a unique position to commit and conceal a fraud, simply because so few others understand IT and how data can be manipulated.

The prior discussion focused mainly on the integrity of data entered into, processed by, and output from the digital environment. However, other risks may be present. For example, the data may accurately go through the system as programmed in the software, but an IT professional periodically substitutes an inappropriate version of the software into the digital environment. Thus, in this example, most transactions are handled correctly and according to system design and company policy; however, some legitimate data are processed by the substituted software and, as a result, are not accurate. Searching for those exceptional transactions requires sifting through the remainder, but it can be approached more effectively with some of the following data extraction and analysis tools.

The IT auditors or assurance professionals need to ensure that they examine the entire control environment, including controls that address other aspects of the computer operation—such as IT operational policies and procedures; data management systems; systems development and integration into the digital environment; system maintenance policies and procedures, including backup and contingency planning; electronic commerce; and daily, weekly, monthly, and annual computer operations—with regard to hardware, software, and IT personnel and user access.

MODULE 2: DIGITAL EVIDENCE

According to the New York Times Peter Henning, "Mishandle a Fraud Search, and All That Fine Evidence Could Be for Nothing[4]." The author observed that