# ACFE Certified Fraud Examiner (CFE) Financial Transactions and Fraud Schemes Practice Exam (Sample)

**Study Guide**

BY EXAMZIFY

**Everything you need from our exam experts!**

**Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.**

# Table of Contents

# Introduction

**Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.**

**This guide was designed to help you do exactly that.**

**Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.**

**The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:**

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

**We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.**

**Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.**

**Let's begin.**

# How to Use This Guide

**This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:**

## 1. Start with a Diagnostic Review

**Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.**

## 2. Study in Short, Focused Sessions

**Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.**

## 3. Learn from the Explanations

**After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.**

## 4. Track Your Progress

**Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.**

## 5. Simulate the Real Exam

**Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.**

## 6. Repeat and Review

**Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.**

**There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!**

# Questions

1. **What type of ratio is the quick ratio?**
   - A. Profitability ratio
   - B. Liquidity ratio
   - C. Solvency ratio
   - D. Efficiency ratio

2. **Which of the following measures is NOT recommended to mitigate billing schemes?**
   - A. Prohibiting competitive bidding
   - B. Providing objective compensation for purchasing staff
   - C. Separating the purchasing and payment functions
   - D. Implementing a fraud hotline

3. **Which of the following would not be a typical red flag for loan fraud when a construction developer submits a draw request?**
   - A. Invoice documentation that appears altered
   - B. Failure to include lien releases from each subcontractor
   - C. Omission of developer's personal account statements
   - D. Missing inspection reports

4. **Which embezzlement scheme involves employees making unauthorized withdrawals from customer accounts?**
   - A. Skimming
   - B. Lapping
   - C. False accounting entries
   - D. Unauthorized withdrawal

5. **Is reconciling cash register totals to cash in the drawer an effective method for detecting cash larceny schemes?**
   - A. Yes
   - B. No
   - C. Only if done weekly
   - D. Only for high-volume stores

6. Which of the following can help prevent a computer from infection by malicious software?

   A. Using anti-malware software.

   B. Installing shareware into a system's root directory.

   C. Updating the operating system regularly.

   D. Updating with the latest security patches.

7. When a change in accounting principle is made, what must be disclosed in the financial statements?

   A. The justification for the change

   B. The historical financial statements

   C. The entity's profit projections

   D. The impact on future earnings

8. What are physical access controls primarily designed to do?

   A. Prevent unauthorized access to computer software

   B. Monitor user behavior online

   C. Prevent unauthorized access to physical locations

   D. Encrypt sensitive digital information

9. What is a common avenue through which proprietary company information can be compromised?

   A. Speeches by executives

   B. Publications

   C. Company website

   D. All of the above

10. What tactic is NOT typically used by fraudsters to physically infiltrate organizations?

   A. Securing a position as an employee

   B. Pose as a contractor

   C. Use of social media to gain information

   D. Fabricate or steal an employee badge

# Answers

1. B
2. A
3. C
4. D
5. B
6. A
7. A
8. C
9. D
10. C

# Explanations

## 1. What type of ratio is the quick ratio?

A. Profitability ratio

B. Liquidity ratio

C. Solvency ratio

D. Efficiency ratio

**The quick ratio is classified as a liquidity ratio, which measures a company's ability to meet its short-term obligations with its most liquid assets. It is calculated by taking current assets, excluding inventories, and dividing that figure by current liabilities. This approach provides a clearer picture of a company's short-term financial health, as it excludes assets that may not be easily converted into cash. Liquidity ratios are essential for assessing a company's capacity to cover its current liabilities without relying on the sale of inventory. The quick ratio specifically highlights how well a firm can address its immediate financial responsibilities using cash or other readily available resources. This makes it a crucial metric for creditors and investors who want to evaluate the short-term financial stability of a business. Profitability ratios, on the other hand, focus on a company's ability to generate income relative to its revenue, assets, or equity. Solvency ratios assess a company's long-term financial viability by evaluating its ability to meet long-term obligations. Efficiency ratios measure how effectively a company utilizes its assets and resources to produce revenue. Therefore, these categories do not accurately describe the objective of the quick ratio.**

## 2. Which of the following measures is NOT recommended to mitigate billing schemes?

A. Prohibiting competitive bidding

B. Providing objective compensation for purchasing staff

C. Separating the purchasing and payment functions

D. Implementing a fraud hotline

**The option that is not recommended to mitigate billing schemes is prohibiting competitive bidding. Competitive bidding is a recognized practice that enhances transparency and fairness in the procurement process. By allowing multiple vendors to submit bids, an organization can obtain the best price and quality for goods and services. This process helps prevent collusion and favoritism, which are key elements of many billing schemes, where vendors might collude with employees to inflate prices or deliver substandard goods. On the other hand, the other measures listed are effective practices for reducing the risk of billing schemes. Objective compensation for purchasing staff ensures that employees are rewarded based on quantifiable performance metrics rather than subjective criteria, reducing the temptation to engage in fraudulent activities for personal gain. Separating the purchasing and payment functions creates a system of checks and balances, making it more difficult for a single employee to commit fraud. Furthermore, implementing a fraud hotline encourages employees to report suspicious activities confidentially, thus promoting a culture of accountability and vigilance against fraudulent activities. Together, these measures create an internal control environment that significantly lowers the risk of billing schemes and enhances overall organizational integrity.**

## 3. Which of the following would not be a typical red flag for loan fraud when a construction developer submits a draw request?

A. Invoice documentation that appears altered

B. Failure to include lien releases from each subcontractor

C. Omission of developer's personal account statements

D. Missing inspection reports

**Omission of the developer's personal account statements is not typically considered a red flag for loan fraud when a construction developer submits a draw request. The focus in evaluating loan fraud usually revolves around the legitimacy and accuracy of the submitted invoices, lien releases, inspection reports, and other documentation directly related to the project and funding draw process. In contrast, the other options are directly linked to common fraud indicators. Altered invoice documentation raises suspicions about the authenticity of costs being claimed. Failure to provide lien releases from subcontractors can indicate potential issues with payments and claims against the property, suggesting that the developer might not be fulfilling their financial obligations. Missing inspection reports can imply that work has not been adequately verified or completed as presented, further signaling possible fraudulent activity. Therefore, the absence of personal account statements does not directly influence the integrity of the construction draw request process, making it the least relevant in identifying loan fraud.**

## 4. Which embezzlement scheme involves employees making unauthorized withdrawals from customer accounts?

A. Skimming

B. Lapping

C. False accounting entries

D. Unauthorized withdrawal

**The embezzlement scheme that specifically involves employees making unauthorized withdrawals from customer accounts is accurately identified as unauthorized withdrawal. This type of scheme occurs when an employee illegally takes money from customer accounts without permission, typically exploiting access to financial systems or direct contact with customers to carry out the unauthorized transactions. Unauthorized withdrawals can lead to significant financial losses for both the customers and the organization. The perpetrator usually covers their tracks by creating false records or manipulating the documentation to hide the missing funds. This method is direct and typically involves actual transfer of funds, making it a straightforward form of embezzlement. In contrast, skimming involves taking cash from a business before it is recorded in the books, which does not specifically relate to customer accounts. Lapping is a technique where an employee takes money from one customer’s account and uses funds from another account to cover it up, creating a cycle of deception. False accounting entries can involve a variety of manipulations but do not necessarily pertain to direct withdrawals from customer accounts. Therefore, unauthorized withdrawal is the most accurate term to describe the action of making unauthorized withdrawals from customer accounts.**

## 5. Is reconciling cash register totals to cash in the drawer an effective method for detecting cash larceny schemes?

A. Yes

B. No

C. Only if done weekly

D. Only for high-volume stores

**Reconciling cash register totals to the cash in the drawer is not considered an effective method for detecting cash larceny schemes primarily because it can easily be manipulated by individuals committing the fraud. When employees are involved in the larceny, they have the power to control the cash register and may alter the records to match the cash they decide to keep for themselves. Because cash larceny involves taking cash that has already been recorded as sales, the discrepancy might not be obvious during a standard reconciliation process. Fraudsters could steal cash while ensuring that the daily register totals appear accurate by manipulating sales records or even utilizing "no sale" transactions to conceal the discrepancy. While regular reconciliations can sometimes reveal inconsistencies and errors, they are not inherently designed to detect cash larceny specifically. The act of reconciling may help to identify discrepancies due to other errors or issues, but it is not a dedicated strategy to uncover internal theft, especially when there is an opportunity for deceitful practices by accomplices within the operation. Thus, in the context of effective fraud detection mechanisms, relying solely on this method would be inadequate against cash larceny schemes. More robust and proactive methods, such as surprise audits, transaction analysis, and segregation of**

## 6. Which of the following can help prevent a computer from infection by malicious software?

A. Using anti-malware software.

B. Installing shareware into a system's root directory.

C. Updating the operating system regularly.

D. Updating with the latest security patches.

**Using anti-malware software is a fundamental and highly effective measure for preventing a computer from being infected by malicious software. This software is specifically designed to detect, prevent, and remove harmful programs such as viruses, worms, trojan horses, and other types of malicious software. By regularly scanning the system, identifying potential threats, and blocking them before they can cause harm, anti-malware software acts as a crucial line of defense against infection. Moreover, while other choices like updating the operating system regularly and applying the latest security patches also contribute to a comprehensive security strategy, they do not directly prevent malicious software in the same proactive and targeted way that dedicated anti-malware solutions do. These updates and patches primarily ensure the operating system remains secure against known vulnerabilities, protecting against potential exploits that could be targeted by malware. Consequently, while both operating system updates and security patches are essential for maintaining broader system security, the active presence of anti-malware software provides direct and continuous protection against a wide range of threats, which is why it is considered a primary defense measure in preventing computer infection by malicious software.**

## 7. When a change in accounting principle is made, what must be disclosed in the financial statements?

**A. The justification for the change**

**B. The historical financial statements**

**C. The entity's profit projections**

**D. The impact on future earnings**

**When a change in accounting principle occurs, it is essential for the financial statements to disclose the justification for that change. This requirement exists because stakeholders and users of the financial statements need to understand the reasons behind the shift in accounting practices. Providing the justification helps them assess the reliability and comparability of the financial information presented. Disclosing the justification allows for greater transparency and helps maintain trust among investors, creditors, and other interested parties. It demonstrates that the entity is adhering to standards and principles that govern accounting practices, thus ensuring that financial reporting remains consistent and understandable. While the historical financial statements, profit projections, and impact on future earnings are important aspects of financial reporting, they are not required disclosures specifically mandated in the context of a change in accounting principle. Instead, focusing on the rationale for the change ensures that users can evaluate its appropriateness and the potential effects it might have on the financial statements as a whole.**

## 8. What are physical access controls primarily designed to do?

**A. Prevent unauthorized access to computer software**

**B. Monitor user behavior online**

**C. Prevent unauthorized access to physical locations**

**D. Encrypt sensitive digital information**

**Physical access controls are primarily designed to prevent unauthorized access to physical locations. These controls include various measures and mechanisms, such as locks, security guards, biometric scanners, and surveillance cameras, which secure buildings, rooms, and other physical spaces where sensitive information or critical infrastructure is housed. By implementing effective physical access controls, organizations can protect their assets, personnel, and confidential data from theft, damage, or compromise. This is crucial because even the most secure digital systems can be undermined by someone gaining physical access to hardware and facilities, allowing them to manipulate or steal information directly. The other options focus on aspects that relate more to cyber security or data protection rather than physical security. For instance, monitoring user behavior online pertains to software and user activity, while encryption relates to securing data rather than controlling physical space. Thus, the importance of physical access controls lies in their ability to safeguard tangible locations against unauthorized access, ensuring a secure environment for operations.**

## 9. What is a common avenue through which proprietary company information can be compromised?

A. Speeches by executives

B. Publications

C. Company website

D. All of the above

**The correct answer is that proprietary company information can be compromised through multiple avenues, including speeches by executives, publications, and the company website. When executives give speeches, they may inadvertently reveal sensitive information while discussing company strategy, future projects, or proprietary technologies. Publications, such as reports, whitepapers, or industry articles, can also disclose valuable insights that competitors could exploit if overly detailed or not properly controlled. Additionally, a company's website is a public platform that might contain important information such as product specifics, market focuses, or financials that can be accessed by anyone, including potential competitors and malicious actors. Each of these methods can lead to unintentional leaks of confidential information, emphasizing the need for companies to be cautious about how they communicate their proprietary knowledge to the public. By recognizing that all listed avenues can contribute to a risk of information loss, one can understand the importance of implementing strong information security practices across various forms of communication.**

## 10. What tactic is NOT typically used by fraudsters to physically infiltrate organizations?

A. Securing a position as an employee

B. Pose as a contractor

C. Use of social media to gain information

D. Fabricate or steal an employee badge

**The use of social media to gain information serves primarily as a tool for gathering intelligence rather than a direct method of physically infiltrating an organization. Fraudsters typically utilize social media platforms to collect personal information about employees, organizational structures, and other sensitive data that could aid in committing fraud. However, this approach does not involve entering the physical premises of an organization or establishing a presence within it. On the other hand, tactics such as securing a position as an employee, posing as a contractor, and fabricating or stealing an employee badge are all methods that directly enable a fraudster to gain physical access to an organization. Securing a legitimate job allows an individual to bypass security protocols. Posing as a contractor provides a similar advantage by allowing fraudsters to exploit vulnerabilities in contractor management processes. Fabricating or stealing an employee badge facilitates unauthorized access into secure areas of the organization. Thus, the direct nature of physical infiltration tactics distinguishes them from the more indirect information-gathering methods that social media usage represents.**

# Next Steps

**Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.**

**As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.**

**If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.**

**Or visit your dedicated course page for more study tools and resources:**

**https://acfecfefintransfraudschemes.examzify.com**

**We wish you the very best on your exam journey. You've got this!**