

Certified Financial Crimes Investigator (CFCI) Practice exam (Sample)

Study Guide



Everything you need from our exam experts!

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright	1
Table of Contents	2
Introduction	3
How to Use This Guide	4
Questions	5
Answers	8
Explanations	10
Next Steps	16

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 added element transformed the Fraud Triangle into the Fraud Diamond?**
 - A. Motivation**
 - B. Opportunity**
 - C. Personal Greed**
 - D. Circumstance**
- 2. What is a common tactic in fraudulent fee reversal?**
 - A. Postponing customer refunds**
 - B. Transferring funds into unauthorized accounts**
 - C. Implementing higher fees without disclosure**
 - D. Offering kickbacks to customers**
- 3. Identity theft refers to which of the following?**
 - A. The stealing of someone's belongings**
 - B. The acquisition of confidential personal information without consent**
 - C. The use of personal data for legitimate transactions**
 - D. The sharing of personal information with others**
- 4. What does loan lapping involve in the context of fraud?**
 - A. Using new loans to pay off old ones**
 - B. Forging loan documents for higher amounts**
 - C. Submitting multiple loan applications**
 - D. Investing loan funds into illegal activities**
- 5. Failure to mark investments to market during market decline can lead to what?**
 - A. Overstating reported liabilities**
 - B. Reducing operational expenses**
 - C. Overstating assets**
 - D. Recording excessive revenues**

- 6. What percentage of people are considered to inherently be dishonest regarding the 20-60-20 rule?**
- A. 10%**
 - B. 20%**
 - C. 30%**
 - D. 40%**
- 7. How does EMV chip technology enhance card security?**
- A. It creates reusable codes for transactions**
 - B. It uses magnetic stripes for data storage**
 - C. It generates unique one-time codes**
 - D. It eliminates the need for passwords**
- 8. What characterizes a case of duplicate payments?**
- A. One invoice leads to multiple payments made to different vendors**
 - B. Two payments issued for the same invoice, one to the vendor and one to a fraudster**
 - C. Payments made for products that were never delivered**
 - D. Checks issued for invalid invoices**
- 9. What kind of information is particularly at risk of being stolen by insiders?**
- A. General public information**
 - B. Company's long-term strategic plans**
 - C. Personally identifiable information (PII) of customers**
 - D. Financial projections**
- 10. What is ACH fraud associated with?**
- A. A person fabricates fake checks**
 - B. A perpetrator uses victim's account information for unauthorized payments**
 - C. An insider steals cash from deposits**
 - D. A person reports false bank transactions**

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What added element transformed the Fraud Triangle into the Fraud Diamond?

- A. Motivation**
- B. Opportunity**
- C. Personal Greed**
- D. Circumstance**

The concept of the Fraud Diamond builds upon the original Fraud Triangle by adding a critical element that reflects a more comprehensive understanding of what drives individuals to commit fraud. The addition of personal greed encapsulates the internal desires and motivations that can influence a person's decision to engage in fraudulent activities. Personal greed acknowledges that beyond just the opportunity and pressure (or motivation), there are individual character traits and psychological factors that can drive someone to act in self-interest, often at the expense of others. The Fraud Triangle highlights three components: opportunity, motivation (or pressure), and rationalization, which explain why a person might commit fraud. By introducing personal greed, the Fraud Diamond expands the framework, emphasizing the importance of understanding the individual motivations that can lead to unethical behavior. This element reflects a deeper insight into the psychological aspects and personal values that may dictate a person's actions in a financial context. Thus, personal greed serves as a crucial layer in understanding the complexities involved in financial crimes, helping investigators to identify and address the nuanced reasons behind fraudulent behaviors.

2. What is a common tactic in fraudulent fee reversal?

- A. Postponing customer refunds**
- B. Transferring funds into unauthorized accounts**
- C. Implementing higher fees without disclosure**
- D. Offering kickbacks to customers**

In the context of fraudulent fee reversal, transferring funds into unauthorized accounts is a tactic that highlights the deceptive nature of such schemes. This approach involves manipulating financial transactions to redirect funds that are supposed to be refunded or reversed, thereby defrauding both the customer and the financial institution. The act of transferring funds into unauthorized accounts often relies on obtaining access to sensitive customer information or exploiting weaknesses in a financial system. By doing this, perpetrators can create financial losses for victims and undermine the integrity of the institution involved. The other options, while they present unethical practices in their own right, do not align as closely with the typical tactics used in fraudulent fee reversal scenarios. For instance, postponing customer refunds might delay the actual return of funds but does not necessarily involve the direct fraudulent use of those funds. Implementing higher fees without disclosure relates to deceptive practices in fee assessment rather than reversing fees. Offering kickbacks to customers constitutes bribery or corruption, which, while illegal, does not specifically address the nuances of fee reversal fraud.

3. Identity theft refers to which of the following?

- A. The stealing of someone's belongings
- B. The acquisition of confidential personal information without consent**
- C. The use of personal data for legitimate transactions
- D. The sharing of personal information with others

Identity theft specifically refers to the acquisition of confidential personal information without consent, enabling a perpetrator to impersonate someone else for fraudulent purposes. This often involves stealing sensitive data such as Social Security numbers, credit card information, or bank account details, which can then be used to commit various forms of fraud, like opening new credit accounts or making unauthorized purchases. The essence of identity theft lies in the unauthorized access and misuse of another person's private information, which clearly correlates with the definition provided in the correct answer. This understanding is crucial for financial crimes investigators, as they must focus on preventing and responding to these types of violations effectively.

4. What does loan lapping involve in the context of fraud?

- A. Using new loans to pay off old ones**
- B. Forging loan documents for higher amounts
- C. Submitting multiple loan applications
- D. Investing loan funds into illegal activities

Loan lapping is a fraudulent scheme typically associated with the manipulation of accounts receivable or loan payments rather than using new loans to pay off old ones. In this context, the act involves deliberately misapplying incoming payments. For instance, an employee may receive payments from one borrower and apply them to the account of another borrower to cover up a shortfall or theft. This creates a cycle where subsequent payments from new borrowers are then used to cover previous borrowers' accounts, creating an illusion of legitimate transactions. The other choices, while related to loan activities, do not accurately represent the essence of loan lapping. Forging loan documents refers to falsifying details to obtain larger loans, which is a different form of financial fraud. Submitting multiple loan applications often involves seeking credit from multiple sources, which may lead to issues of undue credit risk but doesn't specifically involve the manipulation of payments like loan lapping does. Investing loan funds into illegal activities is another form of fraud, typically involving the misappropriation of funds for illicit purposes, rather than the deceptive cycle seen in loan lapping. Overall, loan lapping uniquely captures a sophisticated method of concealing financial discrepancies.

5. Failure to mark investments to market during market decline can lead to what?

- A. Overstating reported liabilities**
- B. Reducing operational expenses**
- C. Overstating assets**
- D. Recording excessive revenues**

When investments are not marked to market during a market decline, it leads to an overstatement of assets. Marking to market refers to the practice of valuing an asset based on its current market price rather than its book value. If the market value of investments declines and they are not adjusted accordingly, this results in the financial statements reflecting a higher asset value than what is realistically achievable in the market. This can create a misleading financial depiction, as stakeholders will believe the institution holds a greater value in assets than it actually does. This oversight can adversely impact investment decisions, risk assessments, and the overall accounting integrity of the organization. The other choices are less relevant in this context: overstating liabilities pertains to inaccurately increasing the value of debits on financial statements; reducing operational expenses is unrelated to asset valuation but rather involves cost management; and recording excessive revenues refers to inaccurate income recognition, which is a separate accounting issue. Therefore, the most accurate consequence of failure to mark investments to market during a decline is overstating assets.

6. What percentage of people are considered to inherently be dishonest regarding the 20-60-20 rule?

- A. 10%**
- B. 20%**
- C. 30%**
- D. 40%**

The 20-60-20 rule is a concept often applied in various fields, including leadership and management, to describe the distribution of behaviors within a group. According to this rule, approximately 20% of people are considered to be inherently dishonest, engaging in unethical or dishonest behaviors more frequently than others. This percentage reflects a consistent observation in social and organizational contexts where a minority demonstrates values or actions that diverge from the norms of honesty and integrity expected in a given environment. The remaining 60% are seen as neutral or adaptable, potentially swaying between honesty and dishonesty depending on circumstances. Meanwhile, the final 20% are characterized as being inherently honest, valuing ethical standards in their decision-making. Understanding this distribution helps professionals in assessing risks and designing strategies for mitigating financial crimes and ethical breaches, as knowing the demographics of honesty versus dishonesty can influence decision-making and policy formulation.

7. How does EMV chip technology enhance card security?

- A. It creates reusable codes for transactions
- B. It uses magnetic stripes for data storage
- C. It generates unique one-time codes**
- D. It eliminates the need for passwords

EMV chip technology significantly enhances card security by generating unique one-time codes for each transaction. This process is referred to as dynamic authentication. When a card is inserted into an EMV-enabled terminal, the chip creates a unique cryptographic code that is specific to that transaction and cannot be reused. This means that even if a criminal were to capture the transaction data, they would not be able to replicate it for future transactions, as the code generated is valid only for that specific instance. In contrast, options that involve reusable codes or magnetic stripes do not provide the same level of security. Magnetic stripes store static data, which can easily be cloned by criminals. Moreover, while the elimination of passwords might streamline the transaction process, this does not directly contribute to the enhanced security measures EMV technology offers. Thus, the unique one-time code generation is a critical aspect of how EMV chip technology improves security for card transactions.

8. What characterizes a case of duplicate payments?

- A. One invoice leads to multiple payments made to different vendors
- B. Two payments issued for the same invoice, one to the vendor and one to a fraudster**
- C. Payments made for products that were never delivered
- D. Checks issued for invalid invoices

In the context of financial crimes, a case of duplicate payments is characterized by the issuance of two payments for the same invoice. In this scenario, one payment goes to the legitimate vendor, while the second payment is directed to a fraudster posing as the vendor. This type of fraud exploits the invoicing system, leading to the same invoice being paid twice, but to different recipients—one legitimate and one fraudulent. This emphasizes the critical need for rigorous invoice verification and payment procedures to mitigate the risks associated with duplicate payments. The other choices depict different types of financial discrepancies but do not accurately illustrate the concept of duplicate payments. For instance, payments made to different vendors for the same invoice represent invoicing errors or mismanagement, rather than duplication. Additionally, payments made for products that were never delivered and checks issued for invalid invoices describe issues relating to fraud or poor accounting practices, rather than focusing on the specific problem of duplicate payments.

9. What kind of information is particularly at risk of being stolen by insiders?

- A. General public information**
- B. Company's long-term strategic plans**
- C. Personally identifiable information (PII) of customers**
- D. Financial projections**

Insiders, such as employees or contractors within an organization, often have access to sensitive and confidential information that can be exploited for personal gain or malicious intent. Personally identifiable information (PII) of customers is particularly at risk because it includes data that can be used to identify individuals, such as names, addresses, Social Security numbers, and financial details. The reason PII is specifically vulnerable is that insiders can leverage their trusted position to extract this information without raising suspicion. PII is valuable on the black market, making it a prime target for insiders who may sell the data or use it for identity theft. Additionally, once PII is obtained, it can lead to significant repercussions for the victims and can be extremely damaging to the organization's reputation and customer trust. While the other options also entail sensitive data, PII stands out because it has direct implications for the individuals whose information is compromised, whereas strategic plans and financial projections, while also sensitive, do not carry the same personal consequences for individuals.

10. What is ACH fraud associated with?

- A. A person fabricates fake checks**
- B. A perpetrator uses victim's account information for unauthorized payments**
- C. An insider steals cash from deposits**
- D. A person reports false bank transactions**

ACH fraud, or Automated Clearing House fraud, primarily involves the unauthorized use of individuals' banking information to initiate payments from their accounts. This often occurs when a perpetrator gains access to a victim's account details—such as account numbers or personal identification numbers—and uses that information to execute transactions without the victim's consent. This can result in significant financial losses for the victim, as funds are withdrawn or transferred fraudulently. The other scenarios presented, while they involve fraudulent activities, do not accurately capture the essence of ACH fraud. Fabricating checks pertains to check fraud, which is distinct from the electronic transactions seen in ACH fraud. Insider theft refers to employees misappropriating cash directly from their employer, which is unrelated to the context of ACH transactions. Reporting false bank transactions generally deals with fraudulent claims made to the bank, rather than the unauthorized use of account information to perform transactions, which is the core issue of ACH fraud.

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://certfinancialcrimesinvest.examzify.com>

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