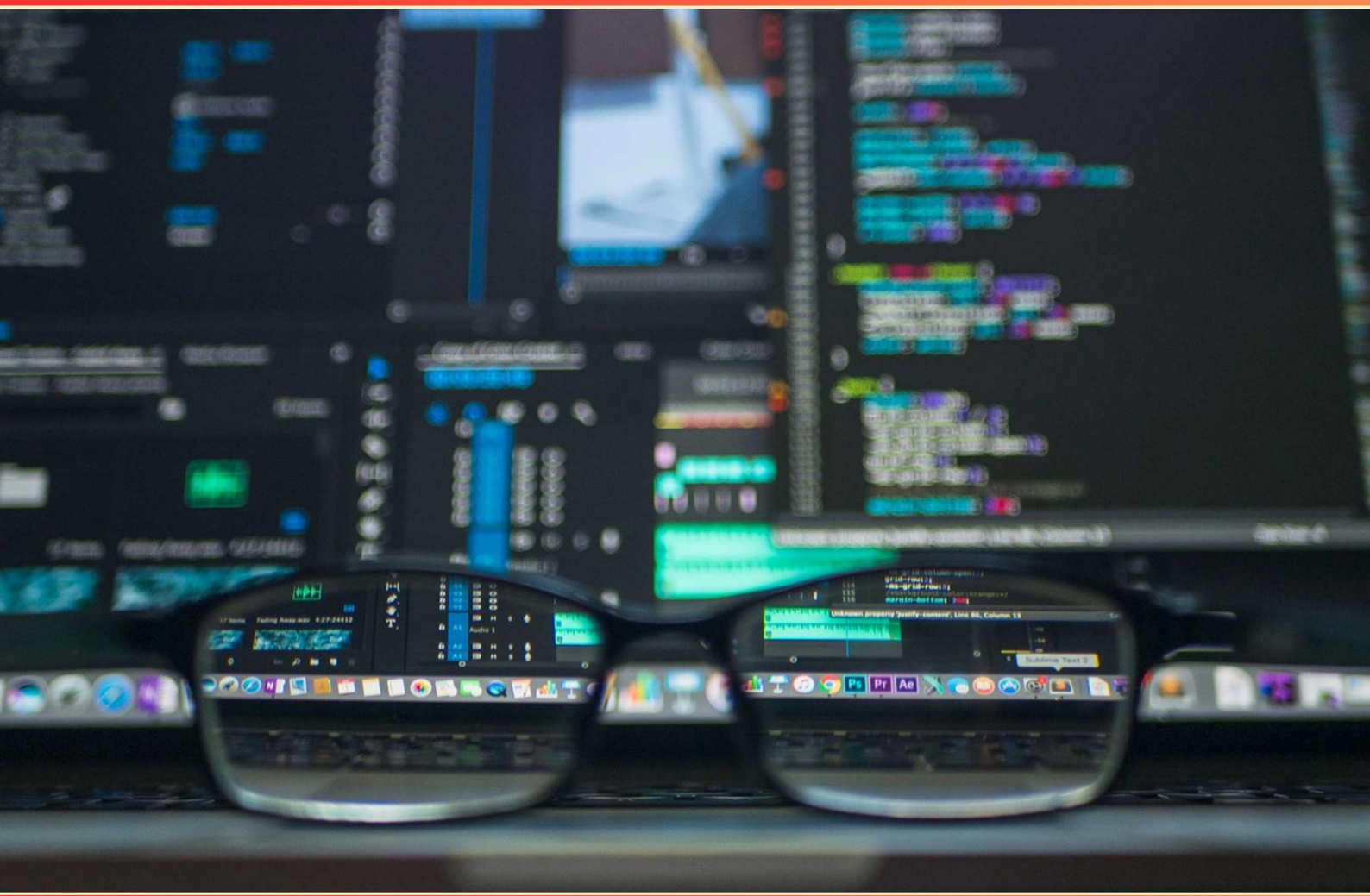
CRYPTOASSET ANTI-FINANCIAL CRIME SPECIALIST (CCAS) CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://
cryptoassetantifinancialcrimespecialist.examzify.com

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What should you do if you forget your login credentials on an online self-hosted wallet?

A. Use your recovery phrase to recover your wallet.

B. Call the number provided by the service provider.

C. Use your other wallets to recover the lost one.

D. Send an email to the service provider.

2. True or False: Some industries are at higher risk for bribery than others, especially those driven by government contracts.

A. True

B. False

C. Depends on the industry

D. Only if international

3. What does the first transaction in a new block show?

A. A payment to the miner for validating transactions.

B. A payment from one person to another.

C. A payment to a node for relaying transactions.

D. A payment by the node to the miner.

4. Which describes an essential process when implementing a new AI tool for transaction monitoring?

A. Conducting regular system updates

B. Training staff on general AI principles

C. Integrating human oversight for algorithm decisions

D. Establishing clear validation and effectiveness measures

5. What is crucial for ongoing AML risk management of a DAO governance token?

A. Total number of tokens in circulation

B. Proportion of tokens held by founders and the development team

C. DAO voting rights attached to each token

D. Whether the token is built on an anonymous or pseudonymous blockchain

SAMPLE

6. What activity is most likely completed when an analyst reviews an Ethereum (ETH) address and observes an approval transaction?

A. Swapped one ETH token for another

B. Minted a non-fungible token

C. Transferred an amount of ETH to a counterparty

D. Gave permission for a contract to access the balance

7. What is the primary difference between a native cryptocurrency and a token?

A. Tokens cannot be exchanged for real-world currency, whereas native cryptocurrency can.

B. Tokens are built on an existing blockchain, whereas cryptocurrency is native to the blockchain.

C. One is backed by real-world value, whereas the other is not.

D. Tokens cannot be used for investment purposes, whereas cryptocurrency can.

8. Which statement is accurate regarding customer due diligence (CDD)?

A. Customer transactions exceeding EUR15,000 should trigger CDD.

B. The non-face-to-face nature of the relationship contributes to the customer risk level.

C. No further CDD is required due to transactional transparency on the blockchain.

D. Only one Financial Action Task Force Recommendation should be applied by VASPs.

9. In blockchain technology, consensus mechanisms are best described as?

A. A validation method for transactions between two wallets.

B. Computers that participate in the competition to solve puzzles.

C. Algorithms that help blockchains synchronize data and remain secure.

D. Nodes in a blockchain network that delegate holdings another node.

10. How are central bank digital currencies (CBDCs) different from stablecoins?

A. CBDCs use blockchain technology.

B. CBDCs hold legal tender status.

C. Stablecoins use more modern technology.

D. Stablecoins are issued by the central monetary authority.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What should you do if you forget your login credentials on an online self-hosted wallet?

A. Use your recovery phrase to recover your wallet.

B. Call the number provided by the service provider.

C. Use your other wallets to recover the lost one.

D. Send an email to the service provider.

Using your recovery phrase to recover your wallet is the appropriate action to take if you forget your login credentials on an online self-hosted wallet. The recovery phrase, often referred to as a seed phrase, is a series of words generated when you create your wallet. It serves as a backup that enables you to regain access to your wallet and its contents in situations where you no longer have your login details. This method of recovery is secure and directly tied to the ownership of the wallet, ensuring that only the rightful owner can regain access. Other choices involve actions that may not result in regaining access to your wallet or could potentially compromise your security. For example, contacting the service provider may not yield results since self-hosted wallets typically do not have centralized support that handles such issues. Similarly, using other wallets or sending an email may not address the core issue of logging in without the appropriate credentials. Therefore, using the recovery phrase is the most reliable and secure approach in this scenario.

2. True or False: Some industries are at higher risk for bribery than others, especially those driven by government contracts.

A. True

B. False

C. Depends on the industry

D. Only if international

The statement is indeed true because certain industries, particularly those that rely heavily on government contracts, do face a heightened risk of bribery. This is often due to the substantial financial stakes involved, as well as the potential for competitive advantages that can be gained through unethical practices. Industries such as construction, defense, and oil and gas are frequently highlighted as particularly vulnerable to bribery because they rely on governmental approvals, permits, and contracts. In these sectors, the interaction between public officials and private companies can create opportunities for corrupt activities, as companies may be willing to offer inducements to secure contracts or favorable treatment. Additionally, the complexity and bureaucratic nature of government procurement processes can further exacerbate the risk of bribery. While other sectors can also be involved in bribery, those with significant government engagement witness higher incidences due to the power dynamics and financial implications at play. Thus, understanding the context of government contracts illuminates why industries in this domain are predisposed to higher bribery risks.

SAMPLE

3. What does the first transaction in a new block show?

A. A payment to the miner for validating transactions.

B. A payment from one person to another.

C. A payment to a node for relaying transactions.

D. A payment by the node to the miner.

The first transaction in a new block typically represents a payment to the miner as a reward for validating and confirming the transactions within that block. This payment is known as the block reward and is an incentive for miners to engage in the resource-intensive process of mining. When a block is successfully mined, the miner receives this reward, which consists of a fixed amount of the cryptocurrency being mined (for example, Bitcoin) as well as any transaction fees included in the transactions that are part of the block. This mechanism is essential for the functioning of many cryptocurrencies, as it not only secures the network but also helps to introduce new coins into circulation. The reward structure encourages miners to contribute their computational power to process and verify transactions, ensuring the integrity and security of the blockchain. In contrast, the other options do not accurately describe the role of the first transaction in a new block. Payments between individuals or transactions involving nodes do not represent the miner's compensation for their work in validating the block. Thus, understanding the significance of the first transaction as a reward for miners is crucial in grasping the incentives built into cryptocurrency systems.

4. Which describes an essential process when implementing a new AI tool for transaction monitoring?

A. Conducting regular system updates

B. Training staff on general AI principles

C. Integrating human oversight for algorithm decisions

D. Establishing clear validation and effectiveness measures

Establishing clear validation and effectiveness measures is essential when implementing a new AI tool for transaction monitoring because it ensures that the AI system is functioning correctly and effectively detecting suspicious activities. This involves defining benchmarks for success, evaluating the system's outputs against these benchmarks, and continuously assessing the tool's performance in real-world scenarios. By doing this, organizations can identify any shortcomings early on, make necessary adjustments to enhance performance, and ensure compliance with regulatory standards. Validation helps in building trust in the AI system's capabilities and enables stakeholders to ascertain that the tool is contributing positively to the organization's overall anti-financial crime strategy. While other processes like training staff or integrating human oversight also hold significance in the overall implementation strategy, they do not inherently guarantee the system's operational success and reliability, which validation specifically addresses.

SAMPLE

5. What is crucial for ongoing AML risk management of a DAO governance token?

A. Total number of tokens in circulation

B. Proportion of tokens held by founders and the development team

C. DAO voting rights attached to each token

D. Whether the token is built on an anonymous or pseudonymous blockchain

For ongoing Anti-Money Laundering (AML) risk management of a Decentralized Autonomous Organization (DAO) governance token, understanding whether the token operates on an anonymous or pseudonymous blockchain is crucial. This consideration reflects the level of transparency available within the blockchain network, which can directly impact the ability to conduct effective AML measures. When tokens are built on anonymous blockchains, they often provide higher levels of privacy for users, making it more challenging to trace transactions and identify potential illicit activities. This lack of transparency can create significant AML risks, as it hinders the ability to monitor for suspicious behavior and confirm the identities of the parties involved in transactions. In contrast, if tokens are built on pseudonymous blockchains, there may be some degree of traceability, helping to mitigate risk by allowing for transaction analysis. The other options, while relevant to understanding the overall structure and distribution of the token, do not directly address the ongoing AML risk management in the same impactful way as the transparency features associated with blockchain anonymity. The total number of tokens in circulation and the proportion held by founders and the development team provide insights into token economics and governance but do not inherently affect the ability to monitor activity for AML purposes. The voting rights attached to each token relate to governance

6. What activity is most likely completed when an analyst reviews an Ethereum (ETH) address and observes an approval transaction?

A. Swapped one ETH token for another

B. Minted a non-fungible token

C. Transferred an amount of ETH to a counterparty

D. Gave permission for a contract to access the balance

When an analyst reviews an Ethereum (ETH) address and observes an approval transaction, it most likely indicates that the individual or entity has given permission for a smart contract to access a specific amount of their tokens. In the context of Ethereum, approval transactions are typically used in token interactions adhering to the ERC-20 standard. They allow a smart contract to transfer tokens on behalf of the user, thus facilitating various operations like trading or staking without requiring the user to transfer tokens directly every time. This mechanism is crucial for decentralized finance (DeFi) applications where users often interact with smart contracts for liquidity pools, swapping tokens, or other functions that necessitate contract-level permissions to access their tokens. The other activities mentioned, such as swapping tokens, minting NFTs, or transferring ETH, do not specifically correlate with an approval transaction. While these activities may involve permissions, they typically do not initiate with an approval transaction but rather are composed of direct transactions involving the transfer or creation of tokens. Therefore, giving permission for a contract to access the balance aligns directly with the nature of an approval transaction.

SAMPLE

7. What is the primary difference between a native cryptocurrency and a token?

A. Tokens cannot be exchanged for real-world currency, whereas native cryptocurrency can.

B. Tokens are built on an existing blockchain, whereas cryptocurrency is native to the blockchain.

C. One is backed by real-world value, whereas the other is not.

D. Tokens cannot be used for investment purposes, whereas cryptocurrency can.

The primary difference between a native cryptocurrency and a token is that tokens are built on an existing blockchain, while native cryptocurrencies are inherent to their own blockchain. Native cryptocurrencies, like Bitcoin or Ether, operate on their respective blockchains and are integral to the functioning of that blockchain, providing the necessary infrastructure for transactions, smart contracts, and security. On the other hand, tokens are created on existing blockchains through standardized protocols (such as ERC-20 for Ethereum) and represent various assets or utilities that can operate within that blockchain's environment. This distinction is crucial for understanding the broader crypto ecosystem, as it highlights how various digital assets interact with blockchain technology in different ways.

8. Which statement is accurate regarding customer due diligence (CDD)?

A. Customer transactions exceeding EUR15,000 should trigger CDD.

B. The non-face-to-face nature of the relationship contributes to the customer risk level.

C. No further CDD is required due to transactional transparency on the blockchain.

D. Only one Financial Action Task Force Recommendation should be applied by VASPs.

The accurate statement regarding customer due diligence (CDD) is that the non-face-to-face nature of the relationship contributes to the customer risk level. In the context of anti-financial crime measures, particularly in virtual asset service providers (VASPs), understanding the risk associated with customer relationships is crucial. When a customer is engaged in a non-face-to-face transaction, it becomes more challenging to verify their identity and assess potential risks associated with their activities. Remote interactions may lack the verification that in-person meetings provide, which can heighten the risk of money laundering and other illicit activities. As a result, enhanced CDD measures are often deemed necessary to mitigate these risks for customers who are engaged in non-traditional or remote transactions. The other statements describe inaccuracies in the context of CDD practices. For instance, while certain thresholds for transactions may require additional scrutiny, the specific threshold mentioned is not universally applicable for CDD. Additionally, transactional transparency on the blockchain does not negate the need for ongoing due diligence, as other risk factors must also be assessed. Moreover, multiple Financial Action Task Force (FATF) Recommendations must be considered rather than just one, highlighting the comprehensive approach needed to anti-money laundering and counter-terrorism financing efforts in the crypto asset realm.

SAMPLE

9. In blockchain technology, consensus mechanisms are best described as?

A. A validation method for transactions between two wallets.

B. Computers that participate in the competition to solve puzzles.

C. Algorithms that help blockchains synchronize data and remain secure.

D. Nodes in a blockchain network that delegate holdings another node.

Consensus mechanisms in blockchain technology refer to the algorithms and protocols that enable nodes within the network to agree on the state of the blockchain and validate transactions. This agreement is crucial because blockchains are decentralized, meaning there is no single authority to oversee the validation process. The correct choice highlights the role of consensus mechanisms in synchronizing data across the network while ensuring the integrity and security of the blockchain. This synchronization is essential for maintaining a consistent and tamper-proof record in a distributed environment where multiple parties may have differing views of the data. The other choices focus on different aspects of blockchain but do not capture the comprehensive nature of consensus mechanisms. For instance, simply referring to a validation method for transactions overlooks the broader functionality of maintaining network integrity. Similarly, while competition to solve puzzles is an element of some consensus mechanisms like Proof of Work, it is not representative of all types and does not encompass the overall purpose of consensus in confirming and synchronizing the entire blockchain. Lastly, the idea of nodes delegating their holdings to other nodes pertains more to specific consensus models rather than the general function of all consensus mechanisms.

10. How are central bank digital currencies (CBDCs) different from stablecoins?

A. CBDCs use blockchain technology.

B. CBDCs hold legal tender status.

C. Stablecoins use more modern technology.

D. Stablecoins are issued by the central monetary authority.

Central Bank Digital Currencies (CBDCs) differ from stablecoins primarily in that CBDCs hold legal tender status. This means that CBDCs are issued and regulated by a country's central bank and are recognized by laws as an official form of currency that can be used for transactions, like physical cash. The government backs them, making them a state-sanctioned medium of exchange. On the other hand, stablecoins, while they aim to maintain a stable value typically pegged to a fiat currency, do not have legal tender status. They are generally issued by private entities and may not carry the same regulatory and legal assurances as CBDCs. This distinction is key in understanding the different roles these forms of digital currency play in the economy and the level of consumer protection and trust associated with them. While CBDCs may utilize blockchain technology, this characteristic is not exclusive to them, as stablecoins can also leverage blockchain. Similarly, stablecoins are not necessarily newer or more modern in their underlying technology compared to CBDCs, and stablecoins are not issued by a central monetary authority, which further highlights their separation from CBDCs.

SAMPLE

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://cryptoassetantifinancialcrimespecialist.examzify.com

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

SAMPLE