

CCAS予想試験、CCASテスト難易度



CCAS認定試験はIT業界の新たなターニングポイントの一つです。試験に受かったら、あなたはIT業界のエリートになることができます。情報技術の進歩と普及につれて、ACAMSのCCAS問題集と解答を提供するオンライン・リソースが何百現れています。その中で、Fast2testが他のサイトをずっと先んじてとても人気があるのは、Fast2testのACAMSのCCAS試験トレーニング資料が本当に人々に恩恵をもたらすことができ、速く自分の夢を実現することにヘルプを差し上げられますから。

ACAMS CCAS 認定試験の出題範囲:

トピック	出題範囲
トピック 1	暗号資産とブロックチェーンのためのAML基礎: この試験セクションでは、マネーロンダリング対策（AML）担当者および暗号資産コンプライアンススペシャリストのスキルを評価します。暗号資産とブロックチェーン環境に合わせたAML原則の基礎知識を網羅し、規制の状況、金融犯罪の類型、そして暗号資産に関連するリスクの進化について解説します。
トピック 2	暗号資産とブロックチェーンのリスク管理プログラム: このセクションでは、暗号資産セクターに特化したリスク管理フレームワークの開発と実装におけるコンプライアンス・マネージャーとリスク管理担当者の専門知識を評価します。暗号資産関連の金融犯罪リスクの評価、管理策の設計、コンプライアンスの監視、暗号資産エコシステムにおける新たな脅威への適応に関する手順が含まれます。
トピック 3	暗号資産とブロックチェーン: この分野は、ブロックチェーンアナリストと暗号資産リスクマネージャーを対象としています。暗号資産技術、ブロックチェーンの基礎、そしてそれらの運用特性を理解することに重点を置いています。受講者は、暗号資産の取引フロー、ウォレット、取引所、スマートコントラクト、そしてこれらが金融犯罪防止にもたらす課題について学びます。

>> CCAS予想試験 <<

ACAMS CCASテスト難易度 & CCAS受験料過去問

ACAMS CCAS試験の困難度なので、試験の準備をやめます。実は、正確の方法と資料を探すなら、すべては問題ではありません。我々社はACAMS CCAS試験に準備するあなたに怖さを取り除き、正確の方法と問題集を提供できます。ご購入の前後において、いつまでもあなたにヘルプを与えられます。あなたのACAMS CCAS試験に合格するのは我々が与えるサプライズです。

ACAMS Certified Cryptoasset Anti-Financial Crime Specialist Examination

認定 CCAS 試驗問題 (Q35-Q40):

質問 # 35

The Financial Action Task Force recommends countries require virtual asset service providers to maintain all records of transactions and customer due diligence measures for a minimum of:

- A. 6 months
- B. 7 years
- C. 5 years
- D. 2 years

正解: C

解説:

FATF standards specify that Virtual Asset Service Providers (VASPs) must keep records related to transactions and customer due diligence for at least 5 years after the completion of the transaction or end of the business relationship. This retention period facilitates effective AML investigations and regulatory reviews.

DFSA AML Module aligns with this timeframe, reinforcing that comprehensive record retention supports audit trails and compliance verification.

質問 # 36

Which features are used by anonymity-enhanced cryptoassets to reduce transparency of transactions and identities? (Select Two.)

- A. Automatic mixing
- B. Cryptographic enhancements
- C. Proof-of-stake mining
- D. Secure hashing algorithm 256
- E. MetaMask wallet

正解: A、B

解説:

Anonymity-enhanced cryptoassets employ specific technical features to obfuscate the details of transactions and the identities of users to reduce traceability and increase privacy. These include:

Automatic mixing (B): This refers to mechanisms such as coin mixers or tumblers that combine multiple transactions from different users into one batch and redistribute them, breaking the direct transaction link and obscuring the audit trail.

Cryptographic enhancements (D): Techniques such as zero-knowledge proofs, ring signatures, stealth addresses, and confidential transactions are cryptographic protocols that conceal sender, receiver, and transaction amount information, making the blockchain ledger less transparent.

Other options explained:

Proof-of-stake mining (A) is a consensus mechanism and not related to anonymity features.

Secure hashing algorithm 256 (C) is a cryptographic hash function standard but does not directly enhance anonymity.

MetaMask wallet (E) is a non-custodial wallet used mainly for Ethereum and tokens but is not an anonymity tool.

Reference from official crypto AML guidance and typology papers:

DFSA AML Module and thematic reviews highlight these anonymity techniques as high-risk indicators requiring enhanced due diligence (EDD).

UAE typology papers and FATF virtual asset guidance emphasize the risk posed by anonymity-enhanced cryptoassets using automatic mixing and cryptographic enhancements to circumvent AML controls 【AML/VER25/05-24: Sections 6.4, 7.3; 31.92._TFS_Typology_Paper_Eng_4.pdf】.

質問 # 37

An exchange uses blockchain analytics to identify high-risk wallet clusters. This is an example of:

- A. Custodial control
- B. KYC
- C. Transaction screening
- D. On-chain forensic analysis

正解: D

解説:

On-chain forensic analysis uses blockchain data to detect illicit wallet patterns and cluster associations.

質問 # 38

Which risk category covers threats from ransomware actors demanding payment in cryptoassets?

- A. Counterparty risk
- B. Operational risk
- C. Cyber-enabled financial crime risk
- D. Liquidity risk

正解: C

解説:

Ransomware schemes are categorized as cyber-enabled financial crimes. AML/CFT frameworks require that such risks be assessed and mitigated through blockchain analytics, sanctions screening, and transaction monitoring for known ransomware wallet addresses.

質問 # 39

A customer sends funds to multiple newly created wallets before cashing out via an exchange. This is an example of:

- A. Chain hopping
- B. Dusting
- C. Structuring
- D. Layering

正解: D

解説:

This process is layering, designed to hide the source of funds through multiple new wallets before integration into the financial system.

質問 # 40

.....

Fast2testのIT専門家は多くの受験生に最も新しいACAMSのCCAS問題集を提供するために、学習教材の正確性を増強するために、一生懸命に頑張ります。Fast2testを選ぶなら、君は他の人の一半の努力で、同じACAMSのCCAS認定試験を簡単に合格できます。それに、君がACAMSのCCAS問題集を購入したら、私たちは一年間で無料更新サービスを提供することができます。

CCASテスト難易度: <https://jp.fast2test.com/CCAS-premium-file.html>

- 素敵CCAS | 100%合格率のCCAS予想試験試験 | 試験の準備方法Certified Cryptoasset Anti-Financial Crime Specialist Examinationテスト難易度 □ [www.mogixam.com]に移動し、□ CCAS □を検索して無料でダウンロードしてくださいCCAS資格難易度
- ACAMS CCAS予想試験: Certified Cryptoasset Anti-Financial Crime Specialist Examination - GoShiken テストエンジンシミュレーション □ ➡ www.goshiken.com □で「CCAS」を検索して、無料でダウンロードしてくださいCCAS復習テキスト
- CCAS資格関連題 □ CCAS試験復習赤本 □ CCAS日本語対策問題集 □ ▶ www.mogixam.com ◀を開き、▶ CCAS ◀を入力して、無料でダウンロードしてくださいCCAS資格取得講座
- 100%合格CCAS予想試験と一番優秀なCCASテスト難易度 □ 《 www.goshiken.com 》で使える無料オンライン版□ CCAS □の試験問題CCAS資格難易度
- 100%合格CCAS予想試験と一番優秀なCCASテスト難易度 □ ☀ www.it-passports.com □☀□で「CCAS」を検索して、無料でダウンロードしてくださいCCAS受験トレーニング
- 実際のCCAS予想試験試験-試験の準備方法-素敵なCCASテスト難易度 □ 最新「CCAS」問題集ファイルは⇒ www.goshiken.com ⇐にて検索CCAS資格関連題
- CCAS資格関連題 * CCAS受験トレーニング □ CCAS日本語認定対策 □ 「 www.goshiken.com 」から☀ CCAS □☀□を検索して、試験資料を無料でダウンロードしてくださいCCAS勉強の資料

- [illegible]