

ACAMS CCAS学習関連題 & CCAS試験番号

ACAMS

Certified Cryptoasset AFC Specialist

STUDY GUIDE

Version 1.02



acams.org

BONUS!!! PassTest CCASダンプの一部を無料でダウンロード: <https://drive.google.com/open?id=1bDVZYcrJfjGDU7IcUA4ZiVVt431GpPHJ>

我々のACAMSのCCASソフトはあなたのすべての需要を満たすのを希望します。問題集の全面性と権威性、ACAMSのCCASソフトがPDF版、オンライン版とソフト版があるという資料のバージョンの多様性、購入の前にデモの無料ダウンロード、購入の後でACAMSのCCASソフトの一年間の無料更新、これ全部は我々の誠の心を示しています。

多くの受験生の反応によって、PassTestの模擬試験は全面的で質が高いです。ACAMS試験は難しいですから、参考資料がないなら、試験に合格するのは簡単ではありません。我々の的中率が高くて安いCCAS問題集を利用して試験に気楽に合格することができます。弊社の問題集がありましたら、易く成功できます。

>> ACAMS CCAS学習関連題 <<

CCAS試験の準備方法 | 実用的なCCAS学習関連題試験 | 権威のある Certified Cryptoasset Anti-Financial Crime Specialist Examination試験番号

高い雇用圧力により、ますます多くの人々が雇用の緊張を和らげ、より良い仕事を得たいと考えています。彼らが問題を解決する最善の方法は、PassTestのCCAS認定を取得することです。認定資格は彼らの労働能力の主要なシンボルであるため、CCAS認定資格を所有できれば、仕事を探しているときに競争上の優位性を獲得できます。短時間でCCAS試験問題を取得することが非常に重要であることを認識する人が増えています。また、CCAS試験問題は、夢のような認定を取得するのに役立ちます。

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 2	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。
トピック 3	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。

ACAMS Certified Cryptoasset Anti-Financial Crime Specialist Examination 認定 CCAS 試験問題 (Q23-Q28):

質問 # 23

Which governance function is ultimately responsible for approving AML/CFT policies?

- **A. Board of Directors**
- B. Compliance officer
- C. MLRO
- D. Chief Executive Officer

正解: A

解説:

The Board holds ultimate responsibility for policy approval under DFSA and FSRA AML rules, ensuring senior-level oversight.

質問 # 24

How should an investigator use transaction history to determine whether cryptoassets were previously involved in money laundering?

- A. Assess the identity of the cryptoasset owner.
- **B. Assess the cryptoasset addresses' receiving exposure to illicit activity.**
- C. Assess other assets held by the cryptoasset owner.
- D. Assess the jurisdiction where the transactions took place.

正解: B

解説:

In the context of AML/CFT frameworks for cryptoassets, the investigation of transaction histories involves blockchain analysis tools to trace the flow of funds to and from crypto addresses. Specifically, it is essential to assess whether the addresses involved have had prior exposure to illicit activities such as known darknet marketplaces, ransomware payments, or sanctioned entities. This form of "address screening" helps identify potentially tainted cryptoassets.

The DFSA AML Module and associated guidance emphasize that transaction monitoring for cryptoassets requires analyzing the provenance of funds, not just ownership. While identifying the owner is part of customer due diligence (CDD), the transactional exposure itself reveals laundering risks embedded in the chain of transfers.

Extract from DFSA AML Module and COB Module on Crypto Business Rules:

"Transaction monitoring systems must include blockchain analysis to detect suspicious activity related to crypto tokens, including

tracing transactions against known illicit sources."

"Enhanced due diligence (EDD) is required when a cryptoasset transaction involves addresses or wallets with a history of illicit activity."

"Risk-based approaches must integrate forensic review of transaction histories to assess financial crime risks in crypto asset transfers" 【AML/VER25/05-24: Sections 6.3, 7.3, 13.3; COB/VER45/05-24: Sections 6.13, 15】.

Therefore, assessing the receiving exposure of cryptoasset addresses to illicit activity (Option C) is the most direct and effective method to detect laundering.

質問 # 25

Which blockchain analysis red flag is linked to terrorism financing?

- A. Smart contract creation
- B. Large OTC trades
- C. Microtransactions to donation addresses
- D. Proof-of-Stake staking

正解: C

解説:

Small-value repeated payments to known extremist donation wallets are a terrorism financing indicator noted in FATF typology reports.

質問 # 26

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

正解: B

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 # 27

Which is a primary benefit of blockchain transparency for AML compliance?

- A. Real-time price tracking
- B. Automatic sanctions screening
- C. Ability to trace historical transactions
- D. Reducing market volatility

正解: C

解説:

Blockchain's transparent ledger enables investigators to trace transaction histories indefinitely, aiding ML/TF detection.

質問 # 28

.....

CCAS試験番号: <https://www.passtest.jp/ACAMS/CCAS-shiken.html>

- 2026年PassTestの最新CCAS PDFダンプおよびCCAS試験エンジンの無料共有: <https://drive.google.com/open?id=1bDVZYcrJfjGDU7lcUA4ZiVVt431GpPHJ>