ACAMS.CCAS.v2026-04-02.q34

Exam Code:	CCAS
Exam Name:	Certified Cryptoasset Anti-Financial Crime Specialist Examination
Certification Provider:	ACAMS
Free Question Number:	34
Version:	v2026-04-02
# of views:	114
# of Questions views:	340
https://www.freeqas.com/qa/ACAMS/CCAS/ACAMS.CCAS.v2026-04-02.q34.html	

NEW QUESTION: 1
Which blockchain characteristic makes forensic tracing of transactions possible?
A. Smart contract automation
B. Decentralized governance
C. Immutable public ledger
D. Sharding
Answer: C (LEAVE A REPLY)
Blockchain's immutability ensures that all transactions remain permanently recorded and tamper-proof, enabling blockchain analytics to trace illicit funds. This property is leveraged in crypto forensic investigations and AML monitoring.

NEW QUESTION: 2
A compliance officer at an exchange who is conducting an annual risk assessment identifies an increased volume of transactions to and from unhosted wallets. Based on Financial Action Task Force guidance, which inherent risk rating would be most appropriate for the compliance officer to assign to such activities?
A. Negligible
B. Low
C. Moderate
D. High
Answer: D (LEAVE A REPLY)
The Financial Action Task Force (FATF) guidance on Virtual Assets and Virtual Asset Service Providers (VASPs) explicitly highlights that transactions involving unhosted wallets (wallets not held or controlled by a regulated entity) pose a high inherent risk for money laundering and terrorist financing. This is because unhosted wallets are more difficult to

monitor and control, lack identifiable customer information, and are often exploited for illicit activities.
The DFSA AML Module, aligned with FATF recommendations, mandates that Relevant Persons incorporate this risk into their business-wide risk assessments. The increased volume of transactions to and from unhosted wallets should therefore be assigned a high inherent risk rating to trigger enhanced controls such as enhanced due diligence (EDD) and transaction monitoring.
Supporting extracts include:
FATF Guidance on Virtual Assets (October 2021) states: "Unhosted wallets or transactions with them represent a high risk of ML/TF due to limited or no access to identifying information." DFSA AML Module (AML/VER25/05-24) Section 4.1 & 6.1 on Risk-Based Approach: mandates firms to assess and rate risks posed by customers and products, explicitly including virtual assets and unhosted wallets as high risk.
COB Module also requires heightened controls and disclosures when dealing with transactions involving unhosted wallets【AML/VER25/05-24: Sections 4.1, 6.1, COB/VER45/05-24: Sections 6.13, 15.6】.
Thus, option D (High) is the correct risk rating.

NEW QUESTION: 3
Which risk category best reflects the risks associated with payment methods (e.g., cash, wires, credit cards, virtual assets)?
A. Geographical
B. Customers
C. New technologies
D. Products and services
Answer: (SHOW ANSWER)
The risks posed by different payment methods fall under the products and services risk category because payment methods are specific services and products offered by financial institutions or businesses. This category assesses inherent risks linked to how products are designed and used.
Geographical (A) relates to location risks; customers (B) relates to the nature of customers; new technologies (C) covers emerging tools but payment methods are classified under products/services.

NEW QUESTION: 4
To identify and assess the money laundering risks emerging from virtual assets, countries should ensure that virtual asset service providers are: (Select Two.)
A. Connected with a regulated financial institution.
B. Subjected to AML regulations
C. Maintaining effective monitoring systems.
D. Located in a jurisdiction with increased regulatory expectations

E. Evaluated for beneficial ownership of virtual asset clients

Answer: B,C (LEAVE A REPLY)

To effectively mitigate money laundering risks in the virtual asset sector, countries must ensure that Virtual Asset Service Providers (VASPs) are subject to AML regulations (B), which provide the legal framework for risk-based customer due diligence and reporting suspicious activities. Additionally, VASPs must maintain effective monitoring systems (C) that enable the detection and reporting of suspicious transactions.

While connection to regulated financial institutions (A) and beneficial ownership evaluation (E) are important components of AML frameworks, the foundational requirements per FATF and DFSA guidance focus on regulatory oversight and operational controls. Jurisdictional regulatory expectations (D) influence enforcement but do not replace the need for direct AML regulatory application on VASPs.

NEW QUESTION: 5

Which is the most important consideration when assessing compromise risks when creating a decentralized finance protocol or smart contract?

A. Security token standard

B. Dual authentication protocols

C. Government regulation

D. Code uniqueness

Answer: (SHOW ANSWER)

Code uniqueness is critical because reuse or replication of vulnerable code exposes protocols to known exploits. Unique, well-audited, and secure code minimizes compromise risk in decentralized finance (DeFi) and smart contracts.

Security standards (A), authentication (B), and regulation (C) are important but secondary to the fundamental security of the code itself.

NEW QUESTION: 6

In a blockchain 51% attack, what does 51% refer to?

A. Governance tokens

B. Wallets

C. Computational power required for mining

D. Exchanges

Answer: (SHOW ANSWER)

A 51% attack refers to a situation where a single miner or group controls more than 50% of the blockchain network's computational (hashing) power. This majority control allows them to manipulate the blockchain ledger by double-spending or blocking transactions.

This term is widely recognized in blockchain security contexts and is referenced in typology papers on crypto financial crime risks, including those issued by UAE authorities and FATF.

Supporting extracts:

DFSA AML thematic reviews mention the risk of manipulation and double spending in blockchains susceptible to 51% attacks.
Typology reports on cryptoasset risks highlight computational power concentration as a core vulnerability.
"51% refers to the percentage of total mining power or computational power in the network" is the standard definition across crypto AML/CFT frameworks【31.92._TFS_Typology_Paper_Eng__4.pdf; AMLCFT_Guidance_for_FIs.pdf】.
Thus, C is correct.

NEW QUESTION: 7
Which type of wallet poses the highest AML risk?
A. Exchange hot wallet
B. Custodial wallet
C. Unhosted wallet
D. Multi-signature wallet
Answer: C (LEAVE A REPLY)
Unhosted wallets allow direct user control without third-party oversight, making them harder to monitor and more vulnerable to misuse.

NEW QUESTION: 8
Which level of an organization is ultimately responsible for risk oversight?
A. 1st line compliance team
B. 2nd line compliance team
C. Chief risk officer
D. Board of directors
Answer: D (LEAVE A REPLY)
The ultimate responsibility for risk oversight lies with the Board of Directors. Senior management and the board have the fiduciary and governance duty to ensure that an effective risk management framework, including AML/CFT controls and cryptoasset-specific risks, is in place and functioning properly.
The DFSA GEN Module and AML Module explicitly allocate the highest accountability for compliance and risk oversight to the Board of Directors, while first and second lines support implementation and oversight respectively. The Chief Risk Officer (CRO) supports risk management but the board maintains ultimate accountability.
Key extracts:
GEN Module, Chapter 5: "Responsibility for compliance lies with every member of senior management, with ultimate oversight by the Board." AML Module Section 1.2 & 4.1: "Senior management and Board must ensure appropriate systems and controls for AML/CFT risk management." FATF Recommendation 2 underscores that senior management and boards are accountable for effective AML governance【GEN/VER64/05-24: Chapter 5; AML/VER25/05-24: Sections 1.2, 4.1】.

Thus, D is the correct answer.

NEW QUESTION: 9
Which token type should be considered as carrying the highest risk when assessing the AML risks related to the customer's source of funds?
A. Privacy
B. Stablecoin
C. Platform
D. Security
Answer: (SHOW ANSWER)
Privacy tokens are specifically designed to obfuscate transaction details such as sender, recipient, and amounts, making them inherently high risk for money laundering and terrorist financing. Their anonymity-enhanced features pose significant challenges to AML efforts.
Stablecoins (B), platform tokens (C), and security tokens (D) have varying risk profiles but generally provide more transparency or are subject to regulatory frameworks, reducing inherent AML risk compared to privacy tokens.
FATF and DFSA AML frameworks highlight privacy tokens as a priority for enhanced due diligence and risk mitigation due to their abuse potential.

NEW QUESTION: 10
A virtual asset service provider (VASP) is using public information on the blockchain to trace a wallet address. Which additional step is necessary to identify the owner or controller of that address?
A. Review the wallet address information periodically.
B. Acquire information to connect the wallet address to a natural person.
C. Screen the wallet address for any historical transaction activity.
D. Obtain further information connecting wallet address to virtual asset transactions.
Answer: B (LEAVE A REPLY)
Public blockchain data is pseudonymous, meaning wallet addresses alone do not reveal the owner's identity. To identify the natural person controlling the wallet, the VASP must acquire additional information, typically through customer due diligence (CDD) processes or data obtained from exchanges and counterparties, linking the wallet address to an individual.
Periodic review (A), transaction screening (C), and obtaining transactional data (D) support ongoing monitoring but do not alone establish identity.
AML and FATF guidance emphasize that ownership linkage requires collecting identifying information beyond blockchain data to comply with AML regulations.

NEW QUESTION: 11

In considering particular virtual asset products, services, or activities, which features should be considered by management?

A. Ability for other virtual asset service providers (VASPs) to utilize the service to provide services to their own customers.

B. Ability to mingle funds within wider pools.

C. Regulatory expectations.

D. Transaction volumes.

Answer: (SHOW ANSWER)

Management must consider a comprehensive set of features when evaluating virtual asset products and services, including:

Ability for other VASPs to utilize the service (A): This increases risk exposure as services may be used indirectly by unknown parties.

Ability to mingle funds within wider pools (B): Mixing services or pooled wallets increase anonymity and laundering risk.

Regulatory expectations (C): Management must ensure compliance with all applicable laws and guidelines.

Transaction volumes (D): High transaction volumes can increase operational risk and require enhanced monitoring.

The DFSA AML and COB Modules, as well as FATF guidance, stress that a risk-based approach requires consideration of all these features in product/service risk assessments.

NEW QUESTION: 12

A firm using blockchain analytics finds an address that sent funds through multiple hops before reaching a darknet market wallet. This is an example of:

A. Direct exposure

B. Indirect exposure

C. Mixing

D. Transaction batching

Answer: B (LEAVE A REPLY)

Indirect exposure occurs when funds pass through one or more intermediary wallets before reaching a known illicit destination. This requires enhanced monitoring to capture risks that are not directly linked but are part of the transaction chain.

NEW QUESTION: 13

Which blockchain analysis red flag is linked to terrorism financing?

A. Microtransactions to donation addresses

B. Large OTC trades

C. Proof-of-Stake staking

D. Smart contract creation

Answer: (SHOW ANSWER)

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

NEW QUESTION: 14
A compliance officer is conducting a customer risk review. Which statements represent the highest level of customer risk? (Select Two.)
A. A customer who uses a virtual private network (VPN) connection to access the customer's account
B. A student customer depositing 15,000 USD over a period of a month, using the funds to purchase cryptoassets that are sent to another virtual asset service provider
C. A business customer opting to pay suppliers in cryptoassets
D. A customer receiving cryptoassets daily from another virtual asset service provider located in a foreign jurisdiction which are then sent to a private wallet
E. A customer located in a foreign country donating 10,000 USD worth of cryptoassets to a charity for veterans in the US
Answer: B,D (LEAVE A REPLY)
When determining highest-risk customers under a risk-based approach, firms must consider transaction patterns, jurisdictions, counterparties, and destinations:
B: Large deposits by a student, rapidly converting to crypto and sending to another VASP, suggest potential layering and third-party funding risk.
D: Daily inbound transfers from a foreign VASP to a private (unhosted) wallet indicate consistent high-risk exposure - especially cross-border transactions involving unregulated or weakly regulated jurisdictions.
While VPN use (A) can be a red flag, on its own it is lower risk than significant suspicious fund flows. Paying suppliers in crypto (C) can be legitimate for businesses. A large donation to a charity (E) could be flagged depending on jurisdiction and cause, but is generally less inherently suspicious than B and D unless linked to high-risk entities.
FATF, DFSA, and FSRA AML rules stress that ongoing monitoring should identify these high-frequency, high-value, cross-border crypto flows as priority for Enhanced Due Diligence (EDD) and possible Suspicious Transaction Reports (STRs).

NEW QUESTION: 15
A customer who runs a cryptoasset automated teller machine (ATM) comes into a financial institution and deposits a larger than usual amount. When asked about the deposit, the customer answers there has been broader adoption of cryptoassets in the region where the ATM is located. Which additional information about the business would indicate high risk for money laundering? (Select Two.)
A. The volume and the number of users increase.
B. The cryptoasset ATM supports a variety of cryptoassets.
C. The region is neighboring with a narcotic-producing jurisdiction.
D. The region is located within a high-risk jurisdiction.

E. The cryptoasset ATM was recently licensed.
Answer: (SHOW ANSWER)
Money laundering risk increases if the business operates in or near high-risk jurisdictions (D) or regions associated with narcotics production (C), as these are common sources of illicit funds.
An increase in volume and users (A) or supporting various cryptoassets (B) alone does not necessarily increase ML risk. Recent licensing (E) may indicate regulatory compliance, potentially lowering risk.

NEW QUESTION: 16
Which first step should a VASP take upon detecting repeated transactions to a high-risk wallet?
A. Immediately freeze the account.
B. Conduct internal investigation and enhanced due diligence.
C. Publicly disclose the wallet.
D. Notify all customers.
Answer: B (LEAVE A REPLY)
EDD and internal review determine whether the activity is suspicious before regulatory reporting or freezing actions.

NEW QUESTION: 17
Which of the following are functions of cryptoasset mining? (Select Two.)
A. Generating new cryptoassets
B. Ensuring the security of the network
C. Optimizing and improving the functionality of the network
D. Validating transactions on the blockchain
Answer: (SHOW ANSWER)
Mining generates new cryptoassets (A) by rewarding miners for solving complex cryptographic puzzles. It also validates transactions on the blockchain (D) by confirming and recording them in blocks, ensuring the integrity of the ledger.

While mining indirectly contributes to network security, the core security mechanisms involve consensus protocols beyond mining alone (B). Optimizing network functionality (C) is usually a development task rather than a mining function.

NEW QUESTION: 18
Under FATF guidance, "unhosted wallets" are:
A. Wallets managed by regulated exchanges.
B. Wallets where users control private keys directly.
C. Custodial wallets held by third parties.
D. Wallets with multi-sig security.
Answer: (SHOW ANSWER)
Unhosted wallets are self-custody wallets controlled directly by the user without third-party oversight, posing higher anonymity and AML risks.

NEW QUESTION: 19
Under DIFC AML regulations, enhanced due diligence (EDD) is mandatory when:
A. A customer is a domestic bank.
B. The customer is from a high-risk jurisdiction.
C. The transaction is above USD 1,000.
D. The customer is a retail investor.
Answer: B (LEAVE A REPLY)
EDD is required when dealing with customers or transactions from jurisdictions identified as high-risk for ML/TF. This aligns with FATF Recommendation 19 and local UAE regulations.

NEW QUESTION: 20
Which is the first action a virtual asset service provider (VASP) should take when it finds out that its customers are engaging in virtual asset (VA) transfers related to unhosted wallets and peer-to-peer (P2P) transactions?
A. Allow VA transfers related P2P or unhosted wallets below 1,000 USD or the equivalent amount in local currency, or per defined thresholds in local regulations.
B. Freeze accounts with records of transactions related to P2P transactions or unhosted wallets.
C. Collect and assess the data on transactions related to P2P or unhosted wallets to determine if it is within its risk appetite.
D. Enhance existing risk-based control framework to account for specific risks posed by transactions related to P2P or unhosted wallets.
Answer: (SHOW ANSWER)
Upon identifying customer engagement with unhosted wallets or P2P transfers, the first step a VASP should take is to collect and assess data on such transactions. This

assessment helps determine if these activities fall within the firm's risk appetite and what enhanced controls or actions may be needed.
Immediate account freezing (B) is not the first step without assessment; neither is allowing transfers (A) without risk consideration. Enhancing risk frameworks (D) is important but follows from an initial data-driven risk assessment.
Relevant guidance:
FATF Recommendations and DFSA AML Module require VASPs to maintain a risk-based approach that begins with data collection and risk assessment on unhosted wallet transactions.
The DFSA's 2023 Dear MLRO letters and thematic reviews stress proportionality and evidence-based responses rather than immediate punitive measures.
Enhanced due diligence (EDD) and risk mitigation measures, including potentially freezing accounts, come after assessment of the risk level【AML/VER25/05-24: Sections 4.1, 6.4, 13; 20230406Dear_MLRO_Letter_re_IEMS.pdf】.
Hence, C is the appropriate first action.

NEW QUESTION: 21
Which blockchain feature ensures that once a block is added, it cannot be altered without network consensus?
A. Consensus algorithm
B. Hash immutability
C. Tokenization
D. Peer-to-peer networking
Answer: B (LEAVE A REPLY)
Hash immutability means that altering any transaction would require changing all subsequent blocks and achieving majority consensus. This security property underpins blockchain integrity and forensic traceability, crucial in AML investigations.

NEW QUESTION: 22
What is the most pertinent item for a cryptoasset money services business to include in a suspicious activity report?
A. All types of cryptocurrencies purchased by the subject, including aggregate total of each and fiat currency equivalent
B. The names of every owner of the destination wallet address(es) to which the subject sent transactions during the review period
C. The aggregate total amount of fiat currency used by the subject to purchase cryptocurrency
D. The subject's account onboarding information not otherwise included in the counter-party information section
Answer: (SHOW ANSWER)

SARs should include detailed transactional information to support investigations, including all types and aggregate amounts of cryptocurrencies purchased, along with fiat currency equivalents. This information provides a clear picture of the subject's activity and financial scale.
Owner names of destination wallets (B) may not be available; onboarding info (D) is supplementary, and fiat aggregate totals (C) alone are insufficient.
FATF and DFSA guidance recommend comprehensive transactional data inclusion in SARs to facilitate law enforcement.

NEW QUESTION: 23
Which type of blockchain is jointly operated by multiple pre-approved organizations?
A. Private
B. Public
C. Consortium
D. Hybrid
Answer: C (LEAVE A REPLY)
Consortium blockchains are semi-private networks where governance is shared among authorized participants, offering a balance between decentralization and access control.

NEW QUESTION: 24
How does law enforcement use Suspicious Activity Reports (SARs)? (Select Two.)
A. To identify regulatory failings
B. To produce evidence of money laundering that can be used in court
C. To develop intelligence on new targets
D. To confirm or develop information on existing targets
Answer: (SHOW ANSWER)
Suspicious Activity Reports (SARs) are a critical tool for law enforcement agencies. They are primarily used to develop intelligence on potential new criminal targets and to confirm or expand information about existing investigations. SARs do not serve as direct evidence of money laundering in court but provide leads and context that enable law enforcement to build cases.
The DFSA's thematic reviews and AML guidance clarify that SARs assist in identifying emerging crime patterns and help intelligence units track suspicious transactions over time. They also allow law enforcement to corroborate data from other sources.
SARs help:
Develop intelligence on new targets (C) by revealing previously unknown suspicious behavior.
Confirm or develop information on existing targets (D) by adding transactional data and context.
Identifying regulatory failings (A) is primarily a supervisory function, and SARs themselves are not evidence for prosecution (B) but intelligence inputs.

Therefore, options C and D are correct.

NEW QUESTION: 25
Which scenario most likely indicates active involvement of a customer in scam activities?
A. Indirect receiving from a scam cluster
B. Indirect sending to a scam cluster
C. Direct sending to a scam cluster
D. Direct receiving from a scam cluster
Answer: C (LEAVE A REPLY)
Directly sending to a scam cluster is a strong indicator of active participation rather than passive exposure, triggering SAR obligations.

NEW QUESTION: 26
If a VASP suspects a transaction involves a sanctioned entity, it must:
A. Report only if over USD 10,000
B. File a SAR and freeze assets if required by law
C. Wait for law enforcement confirmation
D. Cancel the customer account immediately without reporting
Answer: B (LEAVE A REPLY)
Sanctions breaches require immediate reporting to competent authorities and freezing of assets where legally mandated.

NEW QUESTION: 27
What is the correct risk assessment equation used in AML/CFT compliance frameworks, including for cryptoasset risk evaluations?
A. Inherent Risk - Control Effectiveness = Residual Risk
B. Inherent Risk - Residual Risk = Control Effectiveness
C. Residual Risk + Control Effectiveness = Inherent Risk
D. Inherent Risk + Control Effectiveness = Residual Risk
Answer: (SHOW ANSWER)
In risk-based AML/CFT programs - including those applied to Virtual Asset Service Providers (VASPs) - risk assessment determines the remaining exposure after applying mitigating measures.
Inherent Risk: The natural level of risk before applying any controls, based on factors like customer profile, transaction patterns, and jurisdiction.
Control Effectiveness: The degree to which implemented controls (e.g., CDD, EDD, sanctions screening, blockchain analytics) reduce risk.
Residual Risk: The risk that remains after controls are applied and is the level an organization must either accept, reduce further, or avoid.
The standard formula is:
Inherent Risk - Control Effectiveness = Residual Risk

This equation is emphasized in FATF's risk-based approach guidance and reinforced in DIFC (DFSA) and ADGM (FSRA) AML rules to ensure ongoing monitoring and governance oversight of remaining risks.

NEW QUESTION: 28
The "indirect exposure" concept in blockchain analytics means:
A. Funds directly linked to illicit addresses.
B. Funds linked via intermediary addresses.
C. Funds sent to OTC brokers.
D. Funds held in a cold wallet.
Answer: B (LEAVE A REPLY)
Indirect exposure refers to connections through one or more hops to illicit addresses. This requires robust transaction chain analysis to detect hidden ML/TF risk.

NEW QUESTION: 29
An analyst at a virtual asset service provider (VASP) that white-labels its exchange solution to other cross-border VASPs is developing a VASP onboarding procedure. Under Financial Action Task Force Recommendation 13, which CDD practices should be applied to such relationships? (Select Three.)
A. Obtain approval from the local supervisory authority
B. Assess the profitability of the VASP relationship
C. Assess the nature and purpose of the VASP relationship
D. Obtain approval from senior management
E. Assess the VASP's supervision and if a license/registration is needed
Answer: C,D,E (LEAVE A REPLY)
FATF Recommendation 13 (Correspondent Banking and Similar Relationships) and its application to VASP-VASP relationships require enhanced due diligence before onboarding. This is because such arrangements carry elevated ML/TF risk, especially in cross-border settings.
Required CDD practices include:
Assess the nature and purpose of the VASP relationship (C): Understand why the relationship is being established and the expected services/products.
Obtain approval from senior management (D): Senior management oversight ensures risk is accepted at the appropriate governance level.
Assess the VASP's supervision and if a license/registration is needed (E): Confirm regulatory oversight, licensing, and compliance with AML/CFT obligations.
Options A and B are not core FATF requirements for CDD in this context - local authority approval may be a domestic regulatory requirement in some countries, but not a FATF baseline, and profitability assessment is a business decision, not an AML measure.

NEW QUESTION: 30

Which statement regarding cryptocurrencies, digital assets, and blockchain is correct?
A. Cryptocurrencies use encryption techniques operating independently from a central bank.
B. Cryptocurrencies and blockchain are the same and are terms used interchangeably.
C. Digital assets can only operate on a blockchain.
D. Cryptocurrencies, blockchain, and digital assets can all be used as a means of payment.
Answer: A (LEAVE A REPLY)
Cryptocurrencies are digital currencies secured by cryptography, operating independently from any central bank or government. Blockchain is the underlying distributed ledger technology supporting cryptocurrencies and other digital assets.
Cryptocurrencies and blockchain are not the same (B). Digital assets can exist off-blockchain (C), such as tokenized assets on centralized databases. While cryptocurrencies can be used as payment, blockchain itself is a technology, not a payment method (D).

NEW QUESTION: 31
Which type of blockchain is jointly operated by multiple pre-approved organizations?
A. Public
B. Consortium
C. Private
D. Hybrid
Answer: B (LEAVE A REPLY)
Consortium blockchains are semi-private networks where governance is shared among authorized participants, offering a balance between decentralization and access control.

NEW QUESTION: 32
Under DIFC AML rules, which governance body must approve the firm's business-wide risk assessment?
A. Compliance department
B. Board of Directors
C. Chief Technology Officer
D. Internal audit team

Answer: B (LEAVE A REPLY)
DFSA AML Module requires the Board to approve and oversee the firm's business-wide risk assessment, ensuring accountability at the highest governance level.

NEW QUESTION: 33
What is the purpose of a security audit in reason to smart contracts?
A. To allow the developer to confirm that the code does not violate copyright
B. To identify any outdated functions or performance issues
C. To Identify bad actors that ace seeking to misuse the smart contract
D. To protect investors' funds by identifying weaknesses in the code or protocol
Answer: (SHOW ANSWER)
The primary purpose of a security audit for smart contracts is to protect investors' funds by identifying vulnerabilities, coding errors, and weaknesses in the smart contract or underlying protocol that could be exploited. This proactive approach helps prevent hacks, exploits, and financial loss.
While performance issues (B) may be noted, the critical concern is security. Identifying bad actors (C) is not within the scope of a code audit but is a broader operational issue. Copyright concerns (A) are unrelated.
AML and crypto governance frameworks underline the importance of security audits to mitigate operational risks in DeFi and other smart contract-based applications.

NEW QUESTION: 34
Which governance function is ultimately responsible for approving AML/CFT policies?
A. MLRO
B. Board of Directors
C. Compliance officer
D. Chief Executive Officer
Answer: B (LEAVE A REPLY)
The Board holds ultimate responsibility for policy approval under DFSA and FSRA AML rules, ensuring senior-level oversight.