

ACAMS.CAMS7.v2026-08-15.q195

Exam Code:	CAMS7
Exam Name:	Certified Anti-Money Laundering Specialist (CAMS7 the 7th edition)
Certification Provider:	ACAMS
Free Question Number:	195
Version:	v2026-08-15
# of views:	104
# of Questions views:	2016
https://www.freecram.net/torrent/ACAMS.CAMS7.v2026-08-15.q195.html	

NEW QUESTION: 1

Which of the following are common indicators of possible money laundering within the securities industry?

(Select Two.)

- A. Engaging in transactions involving nominees or third parties
- B. Allowing fixed income securities to mature
- C. Using brokerage accounts like deposit accounts
- D. Receiving securities into an existing brokerage account following the death of a spouse

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

According to guidelines issued by Basel Committee on Banking Supervision relating to corporate governance principles for banks, what is the role of the board of directors in addressing an institution's AML oversight and governance?

- A. The board of directors should be responsible for overseeing the management of the bank's compliance risk but not involved in establishing a compliance policy that explains the processes by which compliance risks are to be identified and managed throughout the organization.
- B. The board of directors should establish a compliance function and approve the bank's policies for identifying, assessing, monitoring, reporting, and advising on compliance risk.
- C. The compliance function must have sufficient authority, stature, independence, and resources to be effective on its own and should not have access to the board of directors.
- D. The compliance function should report directly to the CEO concerning the bank's compliance with applicable laws, rules, and standards and only update the board of directors on the bank's efforts in managing compliance risk when required.

Answer: ([SHOW ANSWER](#))

The Basel Committee on Banking Supervision (BCBS) requires that the board of directors establish and oversee the compliance function and approve the bank's AML/CTF compliance

policies and procedures, including processes for identifying, assessing, monitoring, and reporting compliance risks.

"The board of directors should establish a compliance function and approve compliance policies and processes for identifying, assessing, monitoring, and reporting compliance risks throughout the organization." (CAMS 6th Edition, Corporate Governance and Oversight; BCBS, Corporate Governance Principles for Banks, Principle 6) References:

CAMS 6th Edition, Governance and Oversight

BCBS: Corporate Governance Principles for Banks (2015)

NEW QUESTION: 3

The Financial Intelligence Unit (FIU) in a country has received a suspicious activity report (SAR) which involves significant suspicious fund transfers, not only within its jurisdiction but also in a foreign country.

Further information is required from the foreign country to determine whether the matter needs to be referred for prosecution locally.

Which of the following statements is true in this scenario?

- A.** It is against international laws on data protection to access information from foreign countries
- B.** Sovereignty of nations means that information cannot be accessed from foreign countries
- C.** Any information related to money laundering can be received from any organization at any time regardless of jurisdiction
- D.** Countries that are members of the Egmont Group can request assistance for information from each other

Answer: ([SHOW ANSWER](#))

Countries that are members of the Egmont Group can securely exchange information between their Financial Intelligence Units (FIUs) to support money laundering and terrorist financing investigations, even when the activity involves multiple jurisdictions.

NEW QUESTION: 4

Which key metric would provide the most valuable data to the senior management of a financial institution about the effectiveness of its AML controls?

- A.** The ratio of true positives to false positives generated by the automated monitoring system
- B.** The number of clients exited for commercial reasons
- C.** The number of money laundering alerts generated by the watchlist screening system
- D.** The number of high-risk customers onboarded each month

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

Which of the following best describes AML/CFT risk identification and assessment for accountants?

(Select Two.)

- A.** Accountants are not required to keep records of business relationships for more than two years
- B.** Drafting a customer acceptance policy can help accountants define customers outside their risk appetite
- C.** When determining transaction and service risk, the jurisdiction where the accountant provides the service is not important
- D.** Due to their small size and limited resources, accountants are allowed to organize AML/CFT risk only as customer risk or transaction/service risk
- E.** Due to the nature of services accountants provide, automated transaction monitoring systems used by financial institutions may not be appropriate

Answer: ([SHOW ANSWER](#))

Accountants are classified as designated non-financial businesses and professions (DNFBPs) under FATF standards and must apply a risk-based approach to AML/CFT compliance.

A customer acceptance policy is a key tool that helps accountants define which clients or engagements fall outside their risk appetite. This supports consistent onboarding decisions and ensures high-risk clients are either subject to enhanced due diligence or declined.

Additionally, due to the nature of accounting services-such as advisory, tax preparation, and financial reporting-traditional automated transaction monitoring systems used by banks are often not appropriate. Instead, accountants rely more heavily on engagement-based risk assessments, client profiling, and professional judgment.

Accountants are subject to record-keeping requirements longer than two years in most jurisdictions, and geographic risk is always relevant when assessing AML/CFT exposure. Risk assessments must be comprehensive and proportionate, not artificially limited.

NEW QUESTION: 6

Which principles of the Egmont Group of Financial Intelligence Units (FIUs) are aimed at maximizing cooperation between FIUs to more effectively combat money laundering? (Select Two.)

- A.** Formal Egmont Group membership requirements ensure a high commitment of the eligible FIUs
- B.** Information exchange should take place informally, without too many formal prerequisites
- C.** It is within an FIU's authority to sign Memorandums of Understanding independently
- D.** Eliminating spontaneous information sharing between FIUs to reduce the burden of excess investigative work
- E.** FIU cooperation should always be channeled through designated intermediaries

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

Which of the following activities are identified by the Financial Action Task Force (FATF) as being potentially indicative of money laundering through the real estate sector? (Select Four.)

- A.** Use of mortgage products

- B. Use of commercial properties inconsistent with stated business purposes
- C. Use of complex loans or credit finance
- D. Use of corporate vehicles or complex ownership structures
- E. Unexplained cash payments
- F. Use of agricultural land in rural areas

Answer: ([SHOW ANSWER](#))

The real estate sector is recognized by FATF as vulnerable to money laundering due to the high value of transactions and the ability to integrate illicit funds into legitimate assets.

Key red flags include the use of commercial properties in ways inconsistent with the declared business purpose, which may indicate the property is being used to park or disguise illicit funds rather than generate legitimate income.

The use of complex loans or credit financing arrangements can be employed to obscure the true source of funds and create artificial legitimacy. Similarly, corporate vehicles and complex ownership structures are frequently used to conceal beneficial ownership.

Unexplained cash payments are among the most common and serious indicators of money laundering in real estate transactions, particularly when inconsistent with the buyer's profile or local market practices.

The mere use of mortgages or agricultural land does not inherently indicate money laundering risk.

NEW QUESTION: 8

How should risk-related issues be addressed to ensure the effectiveness of the three lines of defense model?

- A. Ensure that the second line reviews, monitors, and escalates risk-related issues as needed to senior management while maintaining independent oversight from the third line
- B. Assign risk-related oversight duties to the third line to provide an independent review and address issues more effectively by avoiding conflicts of interest in the first and second lines
- C. Have senior management handle risk-related issues directly when possible because they are ultimately responsible for the organisation's overall risk management strategy
- D. Delegate some risk-related issues to the first line to avoid overwhelming the second line and to ensure operational efficiency

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 9

Financial Intelligence Units (FIUs) help to protect financial integrity by: (Select Two.)

- A. Receiving and analyzing Suspicious Activity Reports (SARs) to detect financial crime
- B. Disseminating information on emerging trends related to money laundering and associated predicate offenses
- C. Assisting financial institutions with designing products and services that lower residual money laundering risk

D. Ensuring financial institutions maintain appropriate AML programs commensurate with their risk profiles

Answer: ([SHOW ANSWER](#))

Financial Intelligence Units (FIUs) play a central role in national and international AML/CFT frameworks.

According to FATF standards, FIUs are responsible for the receipt, analysis, and dissemination of financial intelligence related to suspected money laundering, terrorist financing, and predicate offenses.

One core function of an FIU is receiving and analyzing SARs submitted by financial institutions and other obliged entities. Through analysis of reported information, FIUs identify suspicious patterns, trends, and networks that may indicate financial crime.

Another key function is disseminating intelligence and typologies to competent authorities and, where appropriate, to the private sector. This includes sharing insights on emerging risks, new money laundering methods, and evolving threat trends, which enhances system-wide financial integrity.

FIUs do not design financial products for institutions, nor do they supervise AML programs-that responsibility lies with AML supervisory authorities. Their role is intelligence-focused rather than regulatory or commercial.

NEW QUESTION: 10

The new KYC lead at a bank is particularly focused on enhancing the risk management component of its KYC program and refers to the Basel Committee's customer due diligence (CDD) principles. Which of the following describe key improvements to a KYC program established in the Basel Committee's CDD principles? (Select Two.)

- A.** Increased frequency of training provided to front office employees
- B.** Enhancement of a customer acceptance policy to more clearly identify high-risk customers
- C.** Implementation of a blacklist of correspondent customers with previously detected and investigated suspicious activity
- D.** Enhancement of customer identification procedures to appropriately identify trust, nominee, and fiduciary accounts

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

The UN Security Council's primary role in imposing sanctions is that it has the authority to:

- A.** impose sanctions to maintain or restore international peace and security.
- B.** impose sanctions on countries that lack AML/CFT controls.
- C.** conduct research on and analyze the impacts of sanctions to improve the effectiveness of sanctions regimes.
- D.** impose sanctions on economic targets to maintain or restore financial stability within a country.

Answer: ([SHOW ANSWER](#))

The United Nations Security Council (UNSC) is the only body with the legal authority under international law to impose binding sanctions on countries, entities, or individuals.

"The Security Council's primary function in imposing sanctions is to maintain or restore international peace and security. These sanctions are legally binding on all UN member states." (CAMS 6th Edition, Chapter: International Sanctions and Proliferation Financing; United Nations Charter, Article 41) Incorrect Options:

B: Sanctions may address AML/CFT failings, but the core mandate is international peace/security.

C: The UNSC does not primarily conduct research or impact analysis.

D: The purpose is international peace/security, not only domestic financial stability.

References:

CAMS 6th Edition, International Sanctions

United Nations Charter, Article 41

NEW QUESTION: 12

A law enforcement agency submits several requests to a financial institution.

Which request is legitimate and requires the bank to respond?

- A. Freeze an account in terms of a court order
- B. Produce documents and testimony without a subpoena
- C. Seize privileged documents upon written request
- D. Keep an account open upon verbal request

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

A compliance officer at a financial institution (FI) is reviewing a new client application for a virtual asset service provider (VASP).

Which details should be part of the risk assessment to determine whether the customer falls within the FI's financial crimes risk appetite? (Select Three.)

- A. Whether the VASP's procedures are sufficient for protecting client personally identifiable information
- B. What percentage of the VASP's clients are classified as higher-risk
- C. Which registered institutions act on behalf of the VASP as operators of virtual asset wallets and virtual asset exchange offices
- D. Whether the VASP is utilizing central bank digital currencies
- E. Who the VASP's clients are, including the breakdown of foreign and domestic individuals

Answer: ([SHOW ANSWER](#))

Virtual Asset Service Providers (VASPs) are considered higher-risk customers under FATF guidance due to their exposure to anonymity, speed of transactions, and cross-border activity. When onboarding a VASP, a financial institution must conduct a thorough risk assessment to determine whether the relationship aligns with its financial crime risk appetite.

Understanding the percentage of higher-risk clients served by the VASP is critical, as it indicates the level of exposure to illicit activity and the robustness of the VASP's own risk management practices. A high concentration of higher-risk customers may significantly increase money laundering and terrorist financing risk.

Identifying which registered institutions act on behalf of the VASP, such as wallet providers or exchange operators, is also essential. Reliance on third parties introduces additional risk and requires assessment of those entities' regulatory status and AML controls.

Finally, knowing who the VASP's clients are, including the proportion of foreign versus domestic customers, is a core component of geographic and customer risk analysis. Cross-border exposure often elevates risk due to differing regulatory standards.

Data privacy practices and the use of central bank digital currencies, while relevant operational considerations, are not primary determinants of AML risk appetite decisions.

NEW QUESTION: 14

Under the Egmont Group Principles, information exchange among financial intelligence units (FIUs) should be conducted:

- A. Only if the status of the foreign FIU is related to law enforcement.
- B. With set limits on the amount of financial and administrative information provided.
- C. Without the expectation of reciprocity on how the information will be used.
- D. Freely, spontaneously, and upon request, on the basis of reciprocity.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

Money laundering has social and economic impacts, especially within developing countries. A high volume of money laundering in a country may: (Select Two.)

- A. Dissuade foreign investment.
- B. Reduce confidence in the country's financial sector.
- C. Dissuade government tax incentive programs
- D. Lower the employment rate.
- E. Reduce volatility in exchange and interest rates.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 16

The goal of the Egmont Group of Financial Intelligence Units (FIUs) is to provide a forum for FIUs to:

(Select Three.)

- A. Sign memoranda of cooperation that recognize and allow room for case-by-case solutions to specific problems
- B. Establish an environment to foster trust amongst countries
- C. Securely share sensitive information in the fight against money laundering and the financing of terrorism

D. Propose legislation to combat financial crime, including money laundering and the financing of terrorism

E. Improve global cooperation between FIUs

Answer: ([SHOW ANSWER](#))

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (**447** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 17

A financial institution plans to implement adverse media screening with Artificial Intelligence (AI)/Machine Learning (ML) capabilities During testing, the system produces high volumes of irrelevant news articles for review.

What is the best way to address this issue?

A. Narrow the media sources to avoid unrelated articles

B. Rely on manual filtering by investigators

C. Increase the frequency of updates to media sources

D. Adjust AI/ML models to focus on high-risk keywords/phrases from reputable media sources

Answer: ([SHOW ANSWER](#))

The most effective way to reduce irrelevant results in AI/ML-driven adverse media screening is to fine-tune the models to prioritize high-risk keywords and reliable sources. This improves precision by filtering out noise and directing focus toward content that is more likely to indicate financial crime risk.

NEW QUESTION: 18

What are the common financial crime risks posed to the e-commerce business model? (Select Three.)

A. Buying goods or services using stolen bank card data

B. Committing fraud against the customer by failing to deliver goods or services

C. Abusing online marketplaces to move criminally obtained funds

D. Evading export control regulations

E. Committing bribery and corruption

Answer: ([SHOW ANSWER](#))

E-commerce business models are exposed to several financial crime risks that are clearly identified in Anti- Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulatory

guidance, including publications from the Financial Action Task Force (FATF) and national supervisory authorities.

One key risk is the use of stolen bank card or payment data to purchase goods or services online. E-commerce platforms are particularly vulnerable to card-not-present fraud, where criminals exploit remote payment channels to generate illicit proceeds.

Another common risk is fraud against customers through non-delivery of goods or services. In these cases, fraudulent merchants accept payments without any intention of fulfilling orders. This form of consumer fraud is recognized as a predicate offense to money laundering under AML frameworks.

Additionally, online marketplaces may be abused to move or disguise criminally obtained funds. Criminals may conduct fake transactions, self-purchases, or repeatedly buy and resell goods to legitimize illicit funds. This activity aligns with recognized typologies such as transaction laundering and trade-based money laundering.

Although export control evasion and bribery and corruption are serious financial crimes, they are not typically considered common or inherent financial crime risks specific to standard e-commerce business models in AML/CFT guidance.

NEW QUESTION: 19

Which measures help ensure that the name screening process is effective in identifying potential risk?

(Select Three.)

- A.** Define in policies and procedures the screening scope, frequency, and alert adjudication process
- B.** Identify the most commonly used name screening database in the industry
- C.** Assign a designated person to ensure consistent implementation of screening controls
- D.** Conduct a risk assessment to determine which data attributes to screen, screening frequency, and database selection
- E.** Conduct regular testing to validate that the screening system is performing as expected

Answer: ([SHOW ANSWER](#))

An effective name screening process is a critical component of sanctions and AML compliance. Regulators expect financial institutions to implement strong governance, risk-based design, and ongoing validation.

Clearly defining the screening scope, frequency, and alert adjudication procedures in policies ensures consistency, transparency, and accountability across the organization.

Conducting a risk assessment allows institutions to make informed, proportionate decisions on which data attributes to screen (e.g., names, aliases, addresses), how frequently to screen, and which databases to use.

This aligns with the risk-based approach.

Regular testing and validation ensure that screening systems continue to perform as intended, detect true matches, and minimize false positives or missed hits.

Selecting the most popular database or assigning a single individual for control ownership does not ensure effectiveness and may introduce governance risk.

NEW QUESTION: 20

Trust and company service providers (TCSPs) should address money laundering risk by: (Select Three.)

- A. Establishing dual controls and quality assurance practices when processing transactions for the client
- B. Considering what additional safeguards may be required when client instructions are given through another TCSP located in another jurisdiction
- C. Requiring the client to complete and submit an AML risk self-assessment to the jurisdiction's Financial Intelligence Unit (FIU)
- D. Gathering and recording information from clients to understand the purpose of the legal entity, as well as the identity of managers and ultimate beneficial owners
- E. Establishing procedures to document the basis on which the TCSP will act as a registered officer for the client and retaining records of that involvement
- F. Conducting an onsite evaluation of the client to assess internal controls

Answer: B,D,E (LEAVE A REPLY)

Trust and company service providers (TCSPs) are classified as higher-risk entities under FATF guidance due to their role in forming and managing legal structures. As a result, TCSPs must implement robust AML controls to mitigate misuse for money laundering.

A key requirement is gathering and recording detailed client information, including the purpose of the legal entity and the identity of managers and ultimate beneficial owners (UBOs). This supports effective customer due diligence and transparency.

TCSPs must also apply additional safeguards when relying on instructions from another TCSP, particularly one located in a different jurisdiction. Reliance on intermediaries increases risk and requires enhanced scrutiny.

Additionally, TCSPs should document the basis on which they act as a registered officer and retain records of their involvement. This ensures accountability and traceability in line with record-keeping obligations.

Requiring clients to submit AML self-assessments to an FIU and conducting onsite evaluations are not standard or required practices under AML frameworks.

NEW QUESTION: 21

Which action could be taken by an organization to better understand the threats faced from proliferation financing?

- A. Work with the front-line to understand their strategic growth targets specifically aimed at increasing their market share around military technology and dual-use products
- B. Review the organization's sanction risk assessment to better understand the potential for exposure to Russia and the Democratic People's Republic of Korea

C. Read and analyze the most recent National Proliferation Financing Risk Assessment produced by the relevant body of the organization's jurisdiction

D. Undertake a detailed review of all payment-related transactions to any clients identified as defense contractors, paying special attention to the beneficial owners of those clients

Answer: ([SHOW ANSWER](#))

Analyzing the most recent National Proliferation Financing Risk Assessment from the relevant authority provides an organization with authoritative, up-to-date insights into current threats, high-risk sectors, and jurisdictional exposures, enabling better understanding and mitigation of proliferation financing risks.

NEW QUESTION: 22

A bank notices inconsistent flagging of blockchain transactions due to the lack of standardized payment message formats.

What feature should be prioritized in the transaction screening tool to address this issue?

A. Enhanced sanctions screening for traditional payment messages

B. Periodic manual review of blockchain-related transactions

C. Integration with blockchain analytics providers

D. Rule-based systems focusing only on known wallet addresses

Answer: ([SHOW ANSWER](#))

Blockchain transactions differ fundamentally from traditional payments because they lack standardized messaging formats such as SWIFT MT or ISO 20022. As a result, conventional screening tools may struggle to consistently detect risks.

Integration with blockchain analytics providers allows institutions to enrich raw blockchain data with contextual intelligence, including wallet attribution, transaction flows, exposure to illicit services, sanctions-linked wallets, and typologies such as mixers and tumblers.

This integration enhances consistency, improves risk detection, and supports sanctions and AML obligations specific to virtual assets. Manual review is not scalable, and focusing only on known wallet addresses creates blind spots. Enhancing traditional payment screening does not address blockchain-specific challenges.

NEW QUESTION: 23

Which of the following is a common strategy employed by non-governmental organizations (NGOs) to combat money laundering?

A. Helping Financial Intelligence Units (FIUs) to analyze the suspicious activity reports (SARs)

B. Directly prosecuting money launderers in court

C. Providing financial assistance to governments to strengthen their anti-money laundering efforts

D. Raising awareness about the issue of money laundering and its consequences

Answer: ([SHOW ANSWER](#))

D: NGOs play an important role in raising awareness about money laundering, lobbying for strong AML/CFT laws, and educating the public and stakeholders about the risks and consequences.

"NGOs help combat money laundering primarily through advocacy, education, and raising public and industry awareness."(CAMS 6th Edition, Role of NGOs in AML/CFT) References:
CAMS 6th Edition, Awareness and Advocacy in AML/CFT
FATF, Outreach to NGOs

NEW QUESTION: 24

Which services provided by an accounting firm could be considered as higher risk from a financial crime perspective? (Choose three.)

- A.** Forming a trust on behalf of a customer with a complex setup and acting as a nominee director
- B.** Auditing a firm that provides payroll software to large corporate customers
- C.** Preparing financial statements for a listed or a privately owned firm
- D.** Providing tax advice to an international customer hoping to move their assets out of their home country
- E.** Assisting an offshore corporation from a jurisdiction with no available beneficial owner information to buy property in the UK

Answer: ([SHOW ANSWER](#))

Forming complex trust structures and acting as a nominee director, providing tax advice to clients moving assets across borders, and assisting offshore entities from opaque jurisdictions in acquiring property are all higher-risk services. These activities may facilitate concealment of beneficial ownership, asset flight, or the integration of illicit funds into legitimate systems.

NEW QUESTION: 25

A multinational financial institution (FI) detected suspicious transactions involving shell companies across the United States, Germany, and Singapore, which appeared to be part of a money laundering scheme. The Financial Intelligence Unit (FIU) in Germany initiated a joint investigation with the U.S.

Financial Crimes Enforcement Network (FinCEN) and the Singapore FIU. The investigation faced challenges due to differing legal frameworks, data privacy laws, and procedural requirements.

Which approach would best enhance cooperation between regulatory authorities and law enforcement agencies across these jurisdictions to ensure a successful investigation?

- A.** Relying on each jurisdiction's existing legal frameworks and informal communication channels
- B.** Engaging a third-party consulting firm to mediate between the regulatory authorities and law enforcement agencies in different jurisdictions
- C.** Centralizing the investigation under the jurisdiction with the most stringent AML laws to streamline the process and reduce the complexity of multi-jurisdictional coordination
- D.** Establishing a Mutual Legal Assistance Treaty (MLAT)

Answer: ([SHOW ANSWER](#))

Cross-border money laundering investigations frequently encounter obstacles arising from differences in legal systems, data protection laws, and investigative procedures. International AML/CFT guidance, including FATF recommendations, emphasizes the importance of formal legal cooperation mechanisms to overcome these challenges.

A Mutual Legal Assistance Treaty (MLAT) provides a structured and legally recognized framework for cooperation between jurisdictions. MLATs allow competent authorities to lawfully exchange information, obtain evidence, and coordinate investigative actions while respecting domestic legal requirements and data privacy obligations. This formal mechanism ensures that information shared is admissible and enforceable across jurisdictions.

Relying solely on informal communication channels is insufficient for complex investigations involving sensitive data and legal constraints. Engaging third-party consultants does not address legal barriers and may introduce confidentiality risks. Centralizing an investigation under a single jurisdiction would undermine sovereignty and is not consistent with international cooperation principles.

Therefore, establishing or utilizing an MLAT is the most effective and regulator-aligned approach to enhance cross-border cooperation in complex money laundering investigations.

NEW QUESTION: 26

A legal instrument executed between two nations that governs cross-border information sharing is known as a:

- A. Memorandum of Agreement.
- B. Declaration of Understanding.
- C. Memorandum of Understanding.
- D. Mutual Legal Assistance Treaty.
- E. Request for Urgent Information.

Answer: D (LEAVE A REPLY)

A Mutual Legal Assistance Treaty (MLAT) is a formal agreement between two or more countries that facilitates cooperation in legal and law enforcement matters, including AML investigations.

Option D (Correct): MLATs allow governments to share financial intelligence, request legal assistance, and conduct joint investigations.

Option A (Incorrect): A Memorandum of Agreement (MOA) is typically a non-binding contract used for general business or governmental cooperation.

Option B (Incorrect): A Declaration of Understanding is an informal agreement and does not provide a legal framework for law enforcement cooperation.

Option C (Incorrect): A Memorandum of Understanding (MOU) is often used for informal cooperation but lacks the legal enforceability of an MLAT.

Option E (Incorrect): A Request for Urgent Information is not a recognized international legal instrument.

Best Practices for Cross-Border AML Cooperation:

Use MLATs to request access to financial records in foreign jurisdictions.

Collaborate with Financial Intelligence Units (FIUs) via the Egmont Group.

Leverage FATF's International Cooperation Review Group (ICRG) for guidance.

Reference:

FATF Recommendation 37 (International Cooperation & MLATs)

U.S. Department of Justice MLAT Procedures

NEW QUESTION: 27

Which statement about the extraterritorial reach of US laws and legislation is accurate?

- A.** Section 319(b) of the USA PATRIOT Act extraterritorial reach permits the seizure of funds from a correspondent bank account in the US that have been opened and maintained for the foreign bank
- B.** The Anti-Money Laundering Act of 2020 (AML Act) extraterritorial reach covers all USD transactions throughout the global economy
- C.** The Office of Foreign Assets Control's (OFAC's) economic and trade sanctions may pose extraterritorial risks for financial institutions and businesses outside of the US
- D.** The Bank Secrecy Act (BSA) extraterritorial reach requires that the Travel Rule be applied to all financial institutions globally, including all USD transactions

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 28

Which principle about safeguarding privacy and data should an auditor adhere to when performing an AML investigation?

- A.** AML and Data Protection Privacy laws should not be mutually exclusive.
- B.** Terrorist financing is more relevant in the context of data protection and supersedes laws.
- C.** Countries should clarify where AML and Data Protection Privacy laws are not balanced.
- D.** During evidence gathering, privacy laws are less important than local AML laws.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

A compliance officer at a financial institution has completed an investigation into a high-risk customer's activities and determined that there are strong indications of money laundering. The compliance officer has documented their findings and is ready to recommend offboarding the customer. However, the relationship manager responsible for the customer is resistant to the idea, citing the customer's significant revenue contribution to the institution.

What should the compliance officer do next to ensure the appropriate escalation and decision-making process is followed?

- A.** Escalate the matter to the institution's high-risk client committee, presenting the investigation findings and recommending offboarding while also acknowledging the relationship manager's concerns
- B.** Proceed with offboarding the customer unilaterally based on their investigation findings and anti-money laundering (AML) concerns
- C.** Attempt to persuade the relationship manager to agree with the offboarding recommendation by highlighting the potential reputational and regulatory risks associated with maintaining the relationship

D. Delay the offboarding decision and continue monitoring the customer's activities, waiting for further evidence to solidify the case for termination

Answer: ([SHOW ANSWER](#))

In situations involving significant AML concerns, especially with high-risk clients, the compliance officer must follow proper escalation procedures within the institution. The appropriate course of action is to escalate the matter to a senior governance body, such as a high-risk client committee, which is typically tasked with balancing AML risk against business considerations.

Unilateral offboarding (Option B) may violate internal protocols.

Persuading the relationship manager (Option C) bypasses formal governance.

Delaying action (Option D) risks further exposure to regulatory or reputational damage.

This escalation ensures documented risk-based decision-making and demonstrates to regulators that the institution applies structured and objective AML governance.

Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: Compliance Governance and Risk Escalation Processes- Section: Governance Structures for High-Risk Customers

NEW QUESTION: 30

As emphasized in the Basel Committee guidance for "Sound management of risks related to money laundering and financing of terrorism", the third line of defense, or audit function, should:

- A.** Report to the audit committee of the board of directors to maintain independence.
- B.** Conduct AML audits no less often than every 12 months for consistency in annual reporting.
- C.** Remain independent from expressing opinions on the sufficiency of remediation or action plans to address findings and recommendations.
- D.** Be involved in the day-to-day operations of the AML program to immediately prevent control failures.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

The EU's 6th Anti-Money Laundering Directive (6AMLD):

- A.** Extended AML oversight to crowdfunding platforms and professional football clubs
- B.** Strengthened provisions relating to the accuracy of data submitted to central beneficial ownership registries
- C.** Eliminated the requirement for the European Commission to conduct a risk assessment
- D.** Created a central EU watchdog to combat money laundering

Answer: ([SHOW ANSWER](#))

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CAMS7 dumps with Test Engine here:

Special Discount Code: **freecram**)

NEW QUESTION: 32

Money laundering can have a profound impact on the global economy that includes:

- A. Declining money supplies
- B. Increased sectoral polarization
- C. Increased inflation and low economic growth
- D. Destabilization of legitimate governments

Answer: ([SHOW ANSWER](#))

Money laundering has far-reaching consequences that extend beyond individual institutions and directly affect national and global economic stability. FATF and international bodies consistently highlight that large-scale money laundering can undermine political and economic systems.

One of the most significant impacts is the destabilization of legitimate governments. Money laundering enables organized crime, corruption, and terrorist financing, which can weaken public institutions, distort policy-making, and erode public trust. In extreme cases, criminal organizations gain influence over governments, law enforcement, or key economic sectors.

While money laundering can indirectly affect inflation and growth, it does not directly cause declining money supplies. "Sectoral polarization" is not a standard or widely recognized economic impact in AML literature.

The most consistently recognized systemic consequence is the erosion of governance, rule of law, and institutional integrity.

Therefore, destabilization of legitimate governments is the most accurate and regulator-supported answer.

NEW QUESTION: 33

An oil exploration company based in France does business with oil refineries in Iran, which is subject to comprehensive Office of Foreign Assets Control (OFAC) sanctions.

What type of OFAC sanctions should be imposed against the French company?

- A. Country-based
- B. Sectoral
- C. List-based
- D. Secondary

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 34

A compliance officer is completing a case and has determined that the events do not merit filing a suspicious activity report (SAR).

Which of the following should be included in the case notes to justify not filing a SAR? (Choose two.)

- A. Who made the decision not to file the SAR

- B. Why the officer deemed that the case did not merit filing a SAR
- C. How much money was involved in the case
- D. How the money flowed through the institution
- E. When the unusual activity occurred

Answer: ([SHOW ANSWER](#))

Case notes should document who made the decision and the rationale for not filing the SAR to ensure transparency, support auditability, and demonstrate compliance with regulatory expectations.

NEW QUESTION: 35

The compliance officer at a casino in Taiwan discovers that the casino received multiple cash deposits from a customer just below the Large-Amount Transaction Report (LTR) limit on consecutive days. The customer used three different betting accounts.

What is the appropriate next step?

- A. Contact law enforcement to launch an investigation into the customer's financial activities
- B. Inform the customer their activity is suspicious and request an explanation
- C. Follow internal reporting procedures to escalate the activity as suspicious and report to appropriate authorities
- D. Make a note in the customer's account that the customer's gambling activities are frequently conducted below the reporting limit

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 36

Which ancillary departments or operational areas can play an essential role in supporting a larger organization's Anti-Money Laundering and Economic Sanctions compliance program? (Choose three.)

- A. Accounting
- B. Model risk management
- C. Technology solutions and IT security
- D. Marketing
- E. Fraud risk management

Answer: ([SHOW ANSWER](#))

Accounting can help detect irregular financial patterns, technology solutions and IT security provide systems for monitoring and data protection, and fraud risk management identifies and mitigates suspicious activities - all of which are essential to supporting AML and sanctions compliance programs.

NEW QUESTION: 37

An annual risk assessment includes inherent risk, effectiveness of controls, and residual risk. The inherent risk is assessed as "moderate," and the effectiveness of controls is "less than satisfactory." What would the residual risk conclusion most likely be?

- A. "Medium," because weak controls would result in the residual risk remaining unchanged
- B. "High," because weak controls would result in increased residual risk
- C. "Moderate," because the risk conclusions for specific areas may be increased
- D. "Low," because controls would lower the risk

Answer: [\(SHOW ANSWER\)](#)

Residual risk represents the remaining level of risk after considering the effectiveness of controls. Under a risk-based approach, strong controls reduce risk, while weak or ineffective controls increase it.

In this scenario, the inherent risk is assessed as moderate, meaning the underlying exposure is neither low nor extreme. However, the controls are evaluated as less than satisfactory, indicating that existing measures are not adequately mitigating the identified risks.

When controls are weak, residual risk increases above the inherent risk level, as vulnerabilities remain unaddressed. Regulators expect financial institutions to escalate residual risk ratings and implement remediation plans in such cases.

Therefore, the most likely residual risk conclusion is high, reflecting the combination of moderate inherent risk and ineffective controls. This outcome aligns with AML best practice and regulatory expectations.

NEW QUESTION: 38

Which of the following risk factors are considered by many supervisory authorities as representing a higher inherent risk associated with MSBs? (Select Two.)

- A. The use of new technologies to facilitate the onboarding of customers remotely
- B. The prevalence of international wire transfers
- C. Domestic business with small and medium-sized enterprises
- D. The cash-intensive nature of the services offered
- E. The use of digital channels and traceable payment methods

Answer: B,D [\(LEAVE A REPLY\)](#)

Money Services Businesses (MSBs) are commonly recognized by regulatory and supervisory authorities as having higher inherent AML/CFT risk, particularly due to certain business characteristics.

Option B - The prevalence of international wire transfers:

MSBs often facilitate cross-border transactions, which present a higher money laundering and terrorist financing risk due to challenges in verifying customer identity, the origin of funds, and the end destination- especially when dealing with higher-risk jurisdictions.

Option D - The cash-intensive nature of the services offered:

Many MSBs deal primarily in cash, which increases the risk of anonymous transactions and funds layering, making it harder to trace illicit activity. Cash is the most vulnerable medium for placement of illicit funds into the financial system.

Option A and Option E, while involving modern technologies, can actually reduce risk when implemented with proper controls (e.g., secure digital onboarding and traceable payments enhance auditability).

Option C does not in itself signal high AML risk unless combined with other red flags.
Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: Industry-Specific Risks-
Section: Money Services Businesses (MSBs) and Their Risk Characteristics

NEW QUESTION: 39

According to FinCEN, when a financial institution (FI) identifies a suspicious activity that necessitates suspicious activity report (SAR) filing, the SAR supporting documentation should (Select Two.)

- A. always be limited to account name, account details, and transaction records.
- B. have written policies and procedures to maintain supporting documentation.
- C. include all documents or records that assisted the FI in making the determination that the activity required a filing.
- D. be saved in a single separate file with hard copies stored in a fireproof cabinet.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

The Basel Committee on Banking Supervision published guidelines on the "Sound management of risks related to money laundering and financing of terrorism." With regard to identifying and accepting customers, it recommends that banks: (Select Two.)

- A. Establish policies and procedures for customer due diligence that vary based on risk.
- B. Establish policies and procedures that encourage processing transactions while due diligence information is being established and verified.
- C. Establish policies and procedures to ensure due diligence activities are identical for all customers.
- D. Are prohibited from offering numbered accounts to customers, even if procedures are established to gather and maintain due diligence information.
- E. Establish policies and procedures to identify and verify customers, beneficial owners, and any individuals that can transact on behalf of their customers.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 41

Which of the following are benefits of the latest KYC solutions, including but not limited to digital onboarding, eKYC, digital identity, facial recognition, liveness checks, biometrics, and geolocation? (Choose three.)

- A. Guaranteeing 100% accuracy in regulatory compliance across all jurisdictions
- B. Improving customer satisfaction by offering personalized recommendations
- C. Reducing identity theft effectively
- D. Providing reliable customer authentication to enhance trust
- E. Decreasing the time required for customer authentication

Answer: ([SHOW ANSWER](#))

Modern KYC solutions help reduce identity theft, provide reliable customer authentication to build trust, and shorten authentication times, enhancing both security and efficiency in customer onboarding and ongoing due diligence processes.

NEW QUESTION: 42

There are three types of factors that can be used to authenticate someone ownership, knowledge, and inherent factors.

Which of the following factors falls under inherent factors?

- A. Challenge-response
- B. Fingerprint
- C. Security token
- D. Passphrase

Answer: ([SHOW ANSWER](#))

Fingerprint is an inherent factor because it is a biometric trait - something the user is. Inherent factors rely on physical or behavioral characteristics such as fingerprints, facial recognition, or voice, which are unique to the individual.

NEW QUESTION: 43

From an international standards perspective both the EU and Financial Action Task Force (FATF) consider data sharing a crucial component of effective anti-money laundering measures because data sharing:

- A. allows Financial Intelligence Units (FIUs) to enact sanctions against perpetrators of financial crime
- B. needs to be approved by the Financial Intelligence Unit (FIU) before sharing between financial institutions
- C. helps financial institutions to be more effective in fighting crime with data analysis
- D. promotes financial transparency and protects the integrity of the financial systems

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

Common risks associated with cryptocurrency and convertible virtual currencies include: (Select Three.)

- A. Funds being stolen from other users
- B. Difficulty converting into physical currency
- C. Obscuring the source of illicit funds
- D. Facilitating payment for other illicit activities and goods
- E. Layering transactions to hide the origin of funds derived from illicit activity

Answer: ([SHOW ANSWER](#))

Cryptocurrencies and convertible virtual currencies present several well-documented money laundering and terrorist financing risks, as identified in FATF guidance and national AML

frameworks. These risks largely stem from the pseudonymous nature, speed, and borderless design of virtual asset transactions.

One key risk is the ability to obscure the source of illicit funds. Criminals can move value through wallets and exchanges in ways that make tracing the origin of funds more difficult, particularly when using privacy-enhancing technologies or poorly regulated platforms.

Another significant risk is the facilitation of payments for illicit goods and activities, including drugs, cybercrime services, ransomware, and sanctions evasion. Virtual currencies can be used to settle transactions outside the traditional financial system.

Additionally, criminals frequently engage in layering transactions, rapidly transferring funds across multiple wallets, platforms, or blockchains to hide the origin of illicit proceeds.

Difficulty converting into physical currency is not a recognized AML risk, as most convertible virtual currencies can be exchanged through regulated platforms. Theft of funds is a cybersecurity concern but is not itself a core AML risk indicator.

NEW QUESTION: 45

Which of the following indicators of potentially suspicious activity are commonly associated with high-risk business sectors and structures such as shell companies? (Select Three.)

- A.** Knowing the goods or services, if identified, do not match the profile of the company or the nature of the financial activity
- B.** All payments are in smaller amounts below reporting thresholds but are high when aggregated while still being consistent with standard business practices
- C.** A company regularly conducts large-volume transactions in a medium-risk jurisdiction with longstanding business partners and provides complete documentation and audit trails
- D.** Insufficient or no information is available to identify originators or beneficiaries of funds transfers through searches or direct inquiries
- E.** Payments have no stated purpose, do not reference goods or services, or only reference a contract or invoice number

Answer: ([SHOW ANSWER](#))

Shell companies and other high-risk business structures are commonly associated with money laundering schemes designed to obscure ownership and transaction purpose. FATF guidance identifies several red flags indicative of such misuse.

A mismatch between goods or services and the company's stated business profile suggests fictitious or manipulated transactions. Insufficient information on originators or beneficiaries of funds transfers further increases suspicion, as transparency is a core AML requirement.

Additionally, payments lacking a clear purpose or meaningful description may indicate layering or attempts to conceal illicit activity.

Conversely, well-documented transactions with established partners and legitimate audit trails are indicators of lower risk. While structuring below reporting thresholds can be suspicious, it must also be inconsistent with standard business practices to qualify as a red flag.

NEW QUESTION: 46

Which regulation permits financial institutions, upon providing notice to the US Department of the Treasury, to share information with one another in order to identify and report activities that may involve money laundering or terrorist activity to the federal government?

- A. Regulation (EU) 2024/1624 of the European Parliament
- B. Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases (COSMIC)
- C. USA Patriot Act Section 314(a)
- D. USA Patriot Act Section 314(b)

Answer: (SHOW ANSWER)

USA PATRIOT Act Section 314(b) allows financial institutions to voluntarily share information with one another, after notifying the U.S. Treasury, to identify and report possible money laundering or terrorist financing activities.

Key elements include:

Voluntary participation

Prior notice to FinCEN (part of the U.S. Treasury)

Protection from liability when acting in good faith

Enhanced collaborative detection across institutions

Section 314(a) refers to information sharing between law enforcement and financial institutions, not peer-to-peer sharing.

COSMIC is an initiative in certain jurisdictions like Singapore, not U.S. regulation.

Regulation (EU) 2024/1624 is part of the EU AML framework, not relevant to U.S. institutions.

Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: U.S. Regulatory Framework-
Section: USA PATRIOT Act - Information Sharing under Section 314(b)

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**)

Special Discount Code: freeexam)

NEW QUESTION: 47

Financial institutions (FIs) must use a risk-based approach in customer due diligence (CDD) measures for legal entity clients by:

- A. Understanding and obtaining information about the competition the business relationship could face
- B. Identifying a customer's identity using data and information from the internet and social media
- C. Taking reasonable measures to verify the identity of the beneficial owner
- D. Conducting ongoing analysis of the business relationship's profitability

Answer: C ([LEAVE A REPLY](#))

A core requirement of applying a risk-based approach (RBA) in customer due diligence for legal entity clients is the identification and verification of beneficial ownership. FATF standards require financial institutions to take reasonable measures to identify and verify the identity of the natural persons who ultimately own or control a legal entity.

Understanding beneficial ownership is critical because complex corporate structures can be misused to conceal illicit ownership, launder money, or evade sanctions. The depth of verification required depends on the assessed risk level of the customer, with higher-risk entities requiring enhanced due diligence.

Information such as market competition or profitability is not relevant to AML/CFT risk assessment. While open-source information may support due diligence, relying solely on internet or social media sources is insufficient and inconsistent with regulatory expectations.

Therefore, verifying beneficial ownership is the most essential and regulator-mandated CDD measure under a risk-based approach.

NEW QUESTION: 48

What are the main benefits of implementing explainable artificial intelligence (AI) or machine learning (ML) technologies to improve operational effectiveness within AML/CFT compliance? (Select Two.)

- A.** Identifies AML/CFT risks without the need for human involvement
- B.** Reduces the need for human resources
- C.** Processes and analyzes large data sets more quickly and accurately
- D.** Increases auditability, accountability, and overall good governance

Answer: ([SHOW ANSWER](#))

Explainable artificial intelligence (AI) and machine learning (ML) technologies are increasingly adopted within AML/CFT compliance to enhance effectiveness while maintaining regulatory transparency. Regulators emphasize that explainability and human oversight are essential when using advanced analytics.

One key benefit is the ability to process and analyze large volumes of data quickly and accurately. AML programs must review massive transaction datasets, customer profiles, and behavioral patterns. AI and ML models improve detection capabilities by identifying complex patterns and anomalies that may not be evident through traditional rule-based systems.

Another critical benefit of explainable AI is improved auditability, accountability, and governance. Explainable models allow compliance teams, auditors, and regulators to understand how decisions are made, why alerts are generated, and how risks are assessed. This transparency supports regulatory compliance and model governance requirements.

AI systems are not intended to replace human involvement or eliminate compliance staff. Human judgment remains essential for investigations, decision-making, and regulatory reporting.

NEW QUESTION: 49

The primary objectives of the United Nations in developing sanctions regimes include: (Select Three.)

- A. to force developing nations to adopt liberal or substantive democracies.
- B. to support governments and regimes in the peaceful resolution of conflict.
- C. to punish governments for having weak financial crime controls.
- D. to deter non-democratic and non-constitutional changes within countries.
- E. to support the protection of human rights.

Answer: ([SHOW ANSWER](#))

UN sanctions regimes are not punitive but aim to:

- * B: "Support peaceful resolution of conflicts."
- * D: "Deter non-democratic and unconstitutional changes of government."
- * E: "Promote respect for human rights and humanitarian law." (CAMS 6th Edition, United Nations Sanctions; UN Security Council Mandates) Incorrect:
- * A: The UN does not impose sanctions to force regime type.
- * C: Sanctions are not for punishing weak AML controls.

References:

CAMS 6th Edition, UN Sanctions

UN Security Council, Sanctions Objectives

NEW QUESTION: 50

One of the basic elements of an effective AML/CFT compliance program is:

- A. A system of enterprise risk management
- B. An artificial intelligence-based transaction monitoring system
- C. An independent and skilled audit function
- D. An artificial intelligence-based enhanced due diligence system

Answer: ([SHOW ANSWER](#))

An effective AML/CFT compliance program must include several core elements outlined in FATF recommendations and national regulations. One of these essential elements is an independent and skilled audit function.

The purpose of independent audit is to test and validate the effectiveness of AML controls, identify weaknesses, and ensure compliance with regulatory requirements. Audits must be conducted by qualified personnel who are independent from the day-to-day AML operations to maintain objectivity.

While enterprise risk management frameworks and advanced technologies such as AI can enhance AML programs, they are not mandatory foundational elements. Regulators focus on governance, oversight, and accountability rather than technology sophistication.

An independent audit function ensures continuous improvement and provides assurance to senior management and regulators that the AML program is operating effectively.

NEW QUESTION: 51

Assessing the money laundering risk related to a product within the financial sector includes assessing the:

(Select Two.)

- A. governance arrangements
- B. complexity of the products
- C. results of the last audit
- D. financial status of the business

Answer: ([SHOW ANSWER](#))

Governance arrangements (A): "Sound governance and risk management arrangements are fundamental to assessing and managing ML/TF risk in products and services." (CAMS 6th Edition, Risk-Based Approach for Products and Services) Complexity of the products (B): "Complexity increases risk-products that are highly complex, opaque, or allow for multiple layers or jurisdictions are more vulnerable to misuse for ML/TF." (CAMS 6th Edition, Product Risk Assessment) Incorrect Options:

C: Last audit results inform program effectiveness, not inherent product risk.

D: Business financial status is considered in customer risk assessment, not product risk.

References:

CAMS 6th Edition, Product and Service Risk Assessment

FATF Guidance on Risk-Based Approach for Financial Institutions

NEW QUESTION: 52

Which of the following is a benefit of an institution implementing machine learning to identify suspicious transactions?

- A. Adaptable to new AFC typologies through continuous model training
- B. Completely unbiased and without error through continuous model training
- C. More consistent and reliable detection outcomes
- D. Transparent and easy to explain algorithms for regulator and compliance purposes

Answer: ([SHOW ANSWER](#))

A key benefit of machine learning in identifying suspicious transactions is its adaptability to new anti-financial crime typologies through continuous model training, enabling the system to evolve with emerging threats and patterns.

NEW QUESTION: 53

What is the primary advantage of using a risk-based approach in allocating compliance resources?

- A. It reduces the overall cost of compliance programs.
- B. It eliminates the need for periodic audits of low-risk customers.
- C. It ensures focus on high-risk areas while maintaining operational efficiency.
- D. It standardizes compliance processes across all regions.

Answer: ([SHOW ANSWER](#))

The CAMS 6th Edition highlights that a risk-based approach enables organizations to efficiently allocate compliance resources, focusing efforts on areas presenting the highest risk, thereby ensuring both regulatory compliance and operational effectiveness.

"A risk-based approach allows firms to concentrate resources and controls where the risk of ML/TF is highest, while applying simplified measures to lower-risk areas. This enhances both effectiveness and efficiency." (CAMS 6th Edition, AML Compliance Program: Risk-Based Approach) Incorrect Options:

- * A: Cost savings may occur, but it is not the main advantage.
- * B: Audits may still be required, just less frequently for low-risk customers.
- * D: Risk-based approaches are tailored, not standardized, across regions.

References:

CAMS Study Guide 6th Edition, AML Compliance Program, "Risk-Based Approach" FATF Recommendation 1: Assessing risks and applying a risk-based approach

NEW QUESTION: 54

What are the roles of a government Financial Intelligence Unit (FIU)? (Select Three.)

- A.** Disseminate analysis of suspicious transaction and suspicious activity reports to foreign judicial systems to enhance their anti-money laundering and terrorist financing investigations and prosecutions
- B.** Receive reports of suspicious transactions and suspicious activities from reporting institutions or obliged institutions
- C.** Analyze all suspicious transaction and suspicious activity reports received from reporting institutions or obliged institutions
- D.** Disseminate the analysis of suspicious transaction and suspicious activity reports to local law enforcement agencies and foreign FIUs to combat money laundering
- E.** Investigate and where appropriate prosecute all suspicious transaction and suspicious activity reports received from reporting institutions or obliged institutions

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

Money services business (MSB) customers present the greatest financial crime risks to mitigate if they:

(Select Two.)

- A.** Process the activity of a customer's customer
- B.** Conduct a large volume of low-value transactions
- C.** Require registration
- D.** Often send cross-border transfers

Answer: ([SHOW ANSWER](#))

Money services businesses (MSBs) are considered higher-risk customers under AML/CFT frameworks due to their role in facilitating payment flows and fund transfers. FATF guidance highlights specific characteristics that elevate financial crime risk.

One significant risk arises when MSBs process the activity of their customers' customers. This indirect exposure reduces transparency and makes it more difficult for the financial institution to identify the true originators and beneficiaries of transactions, increasing vulnerability to money laundering and terrorist financing.

Another major risk is frequent cross-border transfers. International transactions introduce geographic risk, particularly when funds move through or to jurisdictions with weaker AML controls or higher financial crime prevalence.

While high volumes of low-value transactions can present monitoring challenges, this characteristic alone does not necessarily represent the greatest risk without additional factors. Registration requirements are a regulatory control, not a risk indicator.

NEW QUESTION: 56

Section 319(a) of the USA PATRIOT Act:

- A.** Provides the U.S. Department of Treasury with the authority to apply graduated, proportionate measures against a foreign jurisdiction, foreign financial organization, type of international transaction, or type of account.
- B.** Requires due diligence, and in certain situations enhanced due diligence (EDD), for foreign correspondent accounts, which includes virtually all account relationships that organizations can have with a foreign financial organization and private banking for non-citizens of the U.S.
- C.** Allows the appropriate federal banking agency to require a financial organization to produce, within 120 hours, records or information related to the organization's AML compliance or related to a customer of the organization or any account opened, maintained, administered, or managed in the U.S. by the financial organization.
- D.** Permits the U.S. Government to seize funds from a correspondent bank account in the U.S. that has been opened and maintained for a foreign bank in the same amount as has been deposited with the foreign bank.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 57

Which criminal activities could possibly serve as a predicate offense to financial crimes or money laundering activity? (Select Three.)

- A.** Assault
- B.** Arson
- C.** Bribery or corruption
- D.** Fraud
- E.** Organized crime or racketeering

Answer: ([SHOW ANSWER](#)**)**

Predicate offenses are crimes that generate proceeds which may subsequently be laundered. FATF standards and national AML laws define a wide range of serious crimes as predicate offenses.

Bribery and corruption are among the most common predicate offenses, often involving large illicit payments that require laundering to disguise their origin. Fraud, including financial, consumer, and corporate fraud, is another primary source of illicit proceeds and is universally recognized as a predicate offense.

Organized crime and racketeering encompass coordinated criminal activities designed to generate ongoing illegal income, making them central predicate offenses under AML frameworks. While arson may be considered a serious crime in some jurisdictions, and assault is generally not associated with financial gain, AML regimes focus primarily on crimes that generate substantial proceeds. Therefore, bribery, fraud, and organized crime are the most consistently recognized predicate offenses across jurisdictions.

NEW QUESTION: 58

Which of the below is a core function of a financial intelligence unit (FIU) as described in FATF Recommendation 29?

- A.** Sponsoring the research and development of advanced technological surveillance tools to be used nationally
- B.** Prosecuting significant cases of money laundering or terrorist financing falling under national jurisdiction
- C.** Sharing real-time criminal intelligence gathered from national law enforcement agencies with the private sector
- D.** Serving as a national center for the collection and analysis of suspicious activity

Answer: (SHOW ANSWER)

FATF Recommendation 29 states that an FIU should serve as a national center for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering and terrorist financing.

"The FIU should serve as a national center for the receipt and analysis of suspicious transaction reports (STRs) and other information relevant to ML/TF, and for the dissemination of the results of that analysis." (CAMS 6th Edition, Role of the FIU; FATF Recommendation 29) References:

CAMS 6th Edition, Financial Intelligence Units

FATF Recommendation 29

NEW QUESTION: 59

According to the Financial Action Task Force (FATF) methodology, which situations would require a financial institution (FI) to consider filing a suspicious activity report?

- A.** A transaction involves funds exchanged from crypto to fiat currencies.
- B.** A FI identifies the payer is a dealer in precious metals or stones.
- C.** A beneficiary of a transaction is a politically exposed person.
- D.** A FI is unable to verify the relevant customer due diligence documents.

Answer: (SHOW ANSWER)

NEW QUESTION: 60

A financial institution is conducting an enterprise-wide risk assessment (EWRA) and has identified a high inherent risk of money laundering associated with its private banking division due to the clientele's high net worth and complex financial structures. However, the institution has implemented robust customer due diligence (CDD) and enhanced due diligence (EDD) procedures, along with sophisticated transaction monitoring systems.

How would these controls impact the assessment of residual risk?

- A.** The residual risk would be significantly reduced due to the effectiveness of the controls in place
- B.** The residual risk would be moderately reduced, but further controls may be necessary to achieve an acceptable level
- C.** The residual risk would remain high due to the inherent nature of the private banking business
- D.** The residual risk would be eliminated entirely because the controls are sufficient to mitigate all potential risks

Answer: (SHOW ANSWER)

In an Enterprise-Wide Risk Assessment (EWRA), residual risk is the level of risk that remains after applying mitigating controls to the inherent risk (the risk present before controls are applied).

In this scenario, the inherent risk is high due to the nature of private banking—high net worth clients, cross-border transactions, complex ownership structures, and high-value financial products. However, the institution has implemented robust CDD and EDD, as well as advanced transaction monitoring systems.

According to the CAMS Study Guide - 6th Edition, when effective and properly implemented controls are in place, they can significantly reduce the residual risk—even in high-risk business areas like private banking.

However, no control framework can eliminate all risk entirely.

Option A is correct: Controls can significantly reduce the residual risk when strong, effective systems and procedures are in place.

Option B is partially true but suggests inadequacy, which is not indicated here.

Option C incorrectly assumes residual risk cannot be lowered even with controls.

Option D is incorrect because residual risk cannot be eliminated entirely.

Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: Enterprise-Wide Risk Assessment (EWRA)- Section: Inherent Risk vs. Residual Risk and the Role of Controls

NEW QUESTION: 61

Which of the following measures is one that the FATF recommends that Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs) take to mitigate risks arising from business relationships with foreign politically exposed persons (PEPs)?

- A.** Require approval from the prudential regulator for entering into or continuing the business relationship

- B.** Establish processes to understand the PEP's source of wealth and the source of funds, and to refresh that understanding on a regular basis
- C.** Subscribe to commercial databases to assist in the detection of PEPs
- D.** Raise transaction monitoring thresholds for PEP accounts in automated systems to account for higher transaction values and complex legal vehicles and financial structures

Answer: ([SHOW ANSWER](#))

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (**447** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 62

Cryptocurrency-related technologies that can be exploited by money launderers include: (Select Two.)

- A.** generative copilots.
- B.** small language models.
- C.** privacy coins.
- D.** crypto-mixers.

Answer: ([SHOW ANSWER](#))

C: Privacy coins (like Monero, Zcash) are designed to obscure transaction details, making tracing difficult.

D: Crypto-mixers (or tumblers) mix potentially identifiable cryptocurrency funds with others, obscuring the source.

"Privacy coins and mixing services are specifically cited as high ML/TF risk tools, enabling greater anonymity."(CAMS 6th Edition, Cryptoassets ML/TF Risks; FATF, Virtual Assets Guidance)

References:

CAMS 6th Edition, Virtual Assets, Privacy Coins, and Mixing Services

FATF, Virtual Assets and VASPs Guidance

NEW QUESTION: 63

Country A's anti-corruption authority has been investigating the movement of potential proceeds of bribery and corruption to Country B and is now preparing to take the case to a local court.

Which method of obtaining the required evidence to prosecute the case would be most effective?

- A.** Use the Egmont Secure Web to obtain the required evidence from Country B's financial intelligence unit

- B. Make an official request directly from the head of Country A's anti-corruption authority to Country B's corresponding law enforcement authority
- C. Make a request for the required evidence using Country A's mutual legal assistance treaty with Country B
- D. Use the International Criminal Police Organization (INTERPOL) network to obtain the required evidence from Country B

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 64

Which of the following is one of the pillars of the EU AML Package adopted in June 2024?

- A. Digital Operational Resilience Act
- B. Anti-Corruption Directive
- C. EU AML Regulation
- D. 7th AML Directive

Answer: C ([LEAVE A REPLY](#))

One of the central pillars of the EU AML Package adopted in June 2024 is the EU AML Regulation. This regulation introduces directly applicable AML/CFT rules across all EU member states, replacing the previous approach where AML directives were transposed into national laws. This shift addresses regulatory fragmentation and strengthens enforcement across borders.

The complete AML Package includes the following four pillars:

EU AML Regulation (directly applicable rulebook)

6th AML Directive (not the 7th)

Establishment of a new EU Anti-Money Laundering Authority (AMLA)

Revised Transfer of Funds Regulation, especially concerning crypto-asset service providers The EU AML Regulation aims to unify and streamline the application of AML/CFT measures across the EU, ensuring a consistent and effective framework.

Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: International AML Standards - Section:

European Union AML Framework and Developments

NEW QUESTION: 65

Which of the following are best practices to raise awareness and train staff regarding the risks related to financial crime? (Select Three.)

- A. Tailor training and offer regular training to all employees
- B. Train outside of daily operations and promote awareness of Compliance
- C. Train core AML topics once per year, at a minimum, to relevant employees
- D. Use a variety of training methods and provide necessary resources to employees
- E. Communicate regularly and measure effectiveness of training

Answer: ([SHOW ANSWER](#))

A robust AML training program should incorporate the following best practices to ensure awareness and ongoing engagement:

Option A - Tailored and regular training:

Training should be risk-based and role-specific, ensuring employees understand how AML applies to their function.

Option D - Variety and resources:

Use of interactive, digital, live, and scenario-based methods keeps training effective and adaptable. Providing materials and resources supports continued learning.

Option E - Communication and measurement:

Ongoing AML awareness campaigns and feedback mechanisms help assess the effectiveness of training and reinforce its importance.

Option B is too vague and not recognized as a best practice.

Option C, while helpful, is not sufficient alone—annual frequency without contextual or tailored content is inadequate.

Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: AML Program Components-
Section:

Training and Awareness Best Practices

NEW QUESTION: 66

Which of the following are red flags pertaining to potentially suspicious transactions by a customer? (Select Three.)

- A. A customer deposits a large number of consecutively numbered money orders.
- B. A customer receives wire transfers from different unknown accounts which are immediately wired onwards to a third party.
- C. A customer requests loans made to local companies or secured by obligations of local banks.
- D. A customer has regular deposits and withdrawals primarily in wire transfers.
- E. A customer withdraws cash in amounts just under the reporting threshold.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 67

The financial industry relies heavily on rules-based approaches to transaction monitoring to detect suspicious activities.

Scenario-based systems use technology and algorithms to identify: (Choose three.)

- A. fraudulent identities involving stolen or manufactured identification.
- B. suspicious behavior involving a transaction that occurs at an unusual time of day.
- C. hidden beneficial owners.
- D. transaction patterns involving transactions that exceed a certain dollar amount.
- E. anomalies involving a transaction that occurs in a location far away from the customer's usual spending patterns.

Answer: B,D,E ([LEAVE A REPLY](#))

Scenario-based systems use algorithms to detect suspicious behaviors, such as transactions occurring at unusual times, those exceeding specified thresholds, or those taking place in

locations inconsistent with a customer's typical activity. These anomalies help identify potential financial crime risks.

NEW QUESTION: 68

The primary objectives of the United Nations in developing sanctions regimes include: (Choose three.)

- A. to force developing nations to adopt liberal or substantive democracies.
- B. to support governments and regimes in the peaceful resolution of conflict.
- C. to punish governments for having weak financial crime controls.
- D. to deter non-democratic and non-constitutional changes within countries.
- E. to support the protection of human rights.

Answer: ([SHOW ANSWER](#))

The United Nations develops sanctions regimes primarily to support the peaceful resolution of conflicts, deter unconstitutional or non-democratic changes in governments, and promote the protection of human rights.

These objectives aim to maintain international peace, security, and uphold global norms.

NEW QUESTION: 69

Which of the following statements is true regarding the 2012 Financial Action Task Force (FATF) 40 Recommendations and/or 11 Immediate Outcomes?

- A. The cornerstone of the 40 Recommendations is the adoption of a risk-based approach by each jurisdiction
- B. Each jurisdiction can reach out to the FATF for private access to the interpretive notes to the 40 Recommendations
- C. The 40 Recommendations have not been updated to reflect the impact of new technology
- D. The 11 Immediate Outcomes are recommendations specific to high-risk jurisdictions requiring enhanced monitoring.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 70

Why is it important to use multiple sanctions lists, such as United Nations (UN), Office of Foreign Assets Control ("OFAC"), and European Union ("EU") lists, in name screening systems?

- A. To avoid sanctions breach related to payments
- B. To avoid onboarding customers previously exited due to true match
- C. To meet international regulatory requirements and identify risks across jurisdictions
- D. To be in line with the risk appetite statement

Answer: ([SHOW ANSWER](#))

Using multiple sanctions lists ensures that financial institutions meet international regulatory obligations and can identify sanctions-related risks across different jurisdictions. This comprehensive approach strengthens compliance and reduces the likelihood of exposure to sanctioned individuals or entities.

NEW QUESTION: 71

A trust and company services provider that offers a variety of services to businesses is approached by a client interested in establishing a new company. The client requests assistance with the incorporation process, a local business address, annual maintenance services, and the designation of individuals to serve in official capacities for the new company.

Which of the following services involves a higher money laundering risk?

- A. Appointing individuals to serve in official capacities of the company
- B. Annual maintenance services
- C. Provision of a local business address
- D. Company incorporation services

Answer: ([SHOW ANSWER](#))

Appointing individuals to serve in official capacities poses a higher money laundering risk because it can be used to obscure the true beneficial ownership and control of the company, making it easier to conceal illicit activities or the identity of those directing the business.

NEW QUESTION: 72

Which of the following are limitations of using search engines to screen adverse media? (Select Three.)

- A. Search engines have limited global language coverage
- B. Search engines provide unstructured data that complicates media analysis
- C. Search results are often inefficient in identifying relevant adverse media
- D. The process is time-consuming and requires significant manual effort
- E. Outcomes can be inconsistent due to varying search engine algorithms

Answer: ([SHOW ANSWER](#))

Adverse media screening is an important component of customer due diligence, but reliance on general search engines presents several limitations recognized by AML practitioners and regulators.

Search engines typically provide unstructured data, which makes it difficult to systematically analyze and document results for compliance purposes. Information may be incomplete, duplicated, or lack context.

The process is also time-consuming and highly manual, particularly for institutions screening large customer populations. Manual reviews increase operational burden and introduce inconsistency and human error.

Additionally, search engine algorithms vary, meaning results can differ depending on timing, location, and personalization, leading to inconsistent outcomes that are difficult to audit or reproduce.

While language coverage and relevance may be challenges, the most critical limitations relate to lack of structure, inefficiency, and inconsistent results.

NEW QUESTION: 73

An adequate organizational policy is: (Choose two.)

- A. up to date and reflects all relevant regulatory developments
- B. signed off by the board of directors and regulators
- C. approved by the clients and third parties
- D. clearly communicated and understood by staff

Answer: ([SHOW ANSWER](#))

An adequate organizational policy must be up to date with all relevant regulatory developments to remain compliant, and it must be clearly communicated and understood by staff to ensure proper implementation and adherence.

NEW QUESTION: 74

An AML analyst at a financial institution is examining an alert generated by the automated transaction monitoring system to determine whether the alert should be escalated to the AML unit for further investigation or whether it can be archived as a false positive.

Which action might be reasonable for the AML analyst to take?

- A. Restrict the client's access to the account
- B. Request information from the relationship manager assigned to the account that caused the alert
- C. Send a request for information to the counterparty bank involved in the transaction that caused the alert
- D. Perform below-the-line testing to ensure the automated monitoring system is operating effectively

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 75

The degree of attraction that a company holds to criminal organizations is influenced by the (Select Two.)

- A. amount of annual fees associated with the jurisdiction.
- B. permissibility of bearer shares.
- C. rules governing the disclosure of beneficial ownership by the jurisdiction.
- D. ease of travel to the jurisdiction.

Answer: ([SHOW ANSWER](#))

The susceptibility of a company or jurisdiction to ML/TF abuse is significantly increased by:

Permissibility of bearer shares (B): "Bearer shares make it easy to hide ownership and control, presenting a major risk for misuse by criminals." (CAMS 6th Edition, Beneficial Ownership and Company Transparency) Rules governing the disclosure of beneficial ownership by the jurisdiction (C): "Weak requirements or loopholes in beneficial ownership disclosure are frequently exploited to conceal criminal involvement in corporate structures." (CAMS 6th Edition, Chapter: Legal Persons and Arrangements) Incorrect Options:

A: High or low fees are not a significant ML/TF risk driver.

D: Ease of travel is unrelated to ML/TF risk related to company structures.

References:

CAMS 6th Edition, Beneficial Ownership and Transparency

FATF Recommendations 24, 25

NEW QUESTION: 76

A financial institution has received complaints about friction in the onboarding process when additional information is requested.

Which potential solutions could help ensure a better customer onboarding experience with reduced friction? (Select Two.)

- A.** Implement internal or external tools that streamline onboarding processes
- B.** Implement new processes only once every three years to ensure consistency
- C.** Ensure consistent training of all employees on new processes, policies, and tools
- D.** Ensure that only team leads or managers have decision-making power

Answer: (SHOW ANSWER)

Customer onboarding is a critical AML/CFT process that must balance regulatory compliance with customer experience. Excessive friction can lead to customer dissatisfaction and abandonment. Implementing internal or external tools-such as digital onboarding platforms, document collection tools, and workflow automation-can significantly streamline information gathering and reduce delays while maintaining compliance standards.

Additionally, consistent training of all employees involved in onboarding ensures that information requests are clear, consistent, and proportionate. Well-trained staff reduce rework, confusion, and unnecessary follow- ups, improving customer trust and efficiency.

Restricting decision-making to managers can slow processes, and delaying updates to processes reduces adaptability to evolving risks and regulatory expectations.

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**

Special Discount Code: freeexam)

NEW QUESTION: 77

An organization is developing a comprehensive anti-money laundering (AML) framework.

Which of the following statements best describes the relationship between AML policies and procedures?

- A.** Policies are broad guidelines. Procedures are detailed instructions for specific processes. Only procedures are mandatory for knowledge and adherence.

B. Policies define the principles of an organization and influence the drafting of procedures. Procedures are detailed instructions for specific processes.

C. Policies are detailed instructions for specific processes. Procedures are an overarching framework.

Neither policies nor procedures are mandatory for knowledge and adherence.

D. Policies are detailed instructions for specific processes. Procedures are an overarching framework. Both policies and procedures are mandatory for knowledge and adherence.

Answer: ([SHOW ANSWER](#))

Policies outline the guiding principles and objectives of an organization's AML framework, setting the tone for compliance. Procedures translate these policies into detailed, actionable steps that staff must follow. Both are essential for effective AML compliance.

NEW QUESTION: 78

Financial crime risk related to the use of "hawalas" can stem from: (Select Two.)

A. difficulty in tracking the originator, recipient, and source of transactions.

B. remote verification of identity by third-party program managers.

C. heavy usage by senior political figures.

D. informal networks used for cross-border transactions outside of the formal banking system.

E. heightened risks of returned transactions.

Answer: ([SHOW ANSWER](#))

A: "Hawala and similar informal value transfer systems are difficult to monitor, making it challenging to identify the originator, recipient, and source of funds." D: "Hawala operates through informal networks for cross-border transfers, often outside the formal banking system, increasing AML/CFT risk." (CAMS 6th Edition, Alternative Remittance Systems; FATF, Guidance on Money Transfer Services) References:

CAMS 6th Edition, Money Transfer and Informal Value Transfer Systems

FATF, Alternative Remittance Systems Guidance

NEW QUESTION: 79

A bank is completing a periodic KYC profile review for a customer that is a small digital marketing company based in New York City.

Which of the following would be a red flag?

A. The account activity includes deposits made in multiple branches around New York City into the same account.

B. The account activity includes frequent purchases of tickets to industry conferences and other events.

C. The account activity includes incoming funds transfers at irregular intervals from small businesses located in New York

D. The account activity includes deposit activity into both savings and checking accounts

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 80

Which of the following scenarios warrants enhanced due diligence (EDD)? (Select Three.)

- A. An existing local league footballer trying to open a bank account with a bank in their local jurisdiction
- B. The current prime minister of a country trying to open a bank account in another country
- C. An individual with a current bank account who resides in one country becoming the ambassador of another country
- D. The former personal secretary to the minister of transport in a low-risk country 25 years ago opening a bank account at a bank in a neighboring low-risk country
- E. A bank located in a higher risk country trying to establish a correspondent-respondent banking relationship with a bank in a lower-risk country

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 81

In which of the following scenarios should the customer be deemed to have an overly complex ownership structure?

- A. A privately held company owned by two individuals whose interests are held by a series of trusts and foundations
- B. A trust set up with two co-trustees, one of whom is the grantor and the other is a corporate service provider
- C. A customer that is owned by two families with the involvement of over a dozen owners within the families
- D. A multinational correspondent bank that has three layers of ownership between it and a publicly traded bank holding company

Answer: ([SHOW ANSWER](#))

AML/CFT guidance from FATF emphasizes that overly complex ownership structures are a key red flag when they appear unnecessary for legitimate business purposes and may be designed to obscure beneficial ownership.

A privately held company owned by two individuals whose interests are held through multiple layers of trusts and foundations represents an unnecessarily complex structure. Trusts and foundations are frequently identified in AML typologies as vehicles that can be misused to conceal the true beneficial owners, especially when layered without clear commercial rationale. This complexity increases the risk of money laundering and necessitates enhanced due diligence. By contrast, a trust with two co-trustees, including the grantor and a professional service provider, is common and not inherently complex. Similarly, family-owned businesses with many shareholders may be complex but are not automatically deemed "overly complex" if ownership is transparent. Multinational banks with layered ownership tied to a publicly traded holding company are also common and subject to regulatory oversight.

Therefore, the use of multiple trusts and foundations without clear justification is the clearest indicator of an overly complex ownership structure.

NEW QUESTION: 82

Which of the options below is an indicator of potential insider activity that may warrant escalation For further investigation?

- A.** A relationship manager advocates for overriding the results of the company's client risk rating model that resulted in a client's high-risk rating.
- B.** An investigator does not complete the automated transaction monitoring system alerts assigned to them before the time required by company procedures.
- C.** A relationship manager makes an exception to company policy and proceeds with onboarding a customer without documenting a passport for customer identification
- D.** An If employee shares information about a firm's risk management framework with employees of other firms at an industry convention.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 83

The supply of goods and services can be vulnerable to corruption within a company, particularly the solicitation and receipt of bribes and kickbacks, because: (Choose two.)

- A.** certain contractors may receive preferential treatment, allowing them opportunities to inflate margins during the tender process
- B.** unsuccessful bidders are informed of decisions and provided detailed justifications for awarding the contracts
- C.** procurement and contracting processes involve the management of the tender process, which may lack sufficient oversight
- D.** bids are solicited and disseminated to a wide audience through advertising and other channels.

Answer: ([SHOW ANSWER](#))

Corruption risks in the supply of goods and services often arise when contractors receive preferential treatment, enabling inflated margins, and when procurement processes lack sufficient oversight, making it easier for bribes or kickbacks to influence tender outcomes.

NEW QUESTION: 84

What is the primary purpose of a risk appetite statement (RAS) in an organization and how should it be effectively communicated and implemented?

- A.** An RAS defines the amount and type of risk an organization is willing to take to achieve its objectives and should be communicated clearly to all stakeholders with corresponding controls implemented
- B.** An RAS is a detailed plan for managing operational risks and does not cover strategic or financial risks
- C.** An RAS is a formal document meant for regulatory compliance that does not influence day-to-day risk management practices within the organization
- D.** An RAS is used to outline the risk tolerance limits to external stakeholders and does not need to be communicated within the organization

Answer: (SHOW ANSWER)

A risk appetite statement defines the amount and type of risk an organization is willing to accept in pursuit of its objectives. It must be clearly communicated to all stakeholders and supported by corresponding controls and processes to ensure it is embedded in day-to-day decision-making and risk management.

NEW QUESTION: 85

What are the primary advantages of using open-source tools in financial crime investigations? (Choose two.)

- A. Partial automation of data collection and analysis
- B. Cost-effective access to a wide range of data
- C. Real-time monitoring of selected transactions and data sources
- D. Ability to conduct investigations with minimal human oversight
- E. Enhanced ability to identify connections across various data sets

Answer: A,B (LEAVE A REPLY)

Open-source tools offer cost-effective access to diverse data sources, making them valuable for financial crime investigations. They also support partial automation of data collection and analysis, reducing manual effort and improving efficiency in identifying suspicious patterns or links.

NEW QUESTION: 86

Which control would be most effective as part of a risk-based approach (RBA) to managing AML/CFT risk for a bank established in the EU that also has a branch in a high-risk third country outside of the EU?

- A. Fully rely on central beneficial owner registry records in the high-risk third country to determine the ultimate beneficial owners of all customers
- B. Apply tailored due diligence measures, based on the level of risk posed by each customer following risk assessment
- C. Monitor every cross-border transaction in real time, flagging all for enhanced scrutiny due to the country risk level
- D. Automatically apply enhanced customer due diligence measures to all customers in the high-risk third- country branch regardless of risk level

Answer: (SHOW ANSWER)

As part of a risk-based approach, the bank should apply tailored due diligence measures based on the assessed risk level of each customer. This ensures resources are focused where they are most needed, rather than applying uniform enhanced measures to all customers, which can be inefficient and unnecessary.

NEW QUESTION: 87

During which process must a country demonstrate to the Financial Action Task Force (FATF) that it has an effective framework to protect the financial system from abuse?

- A. Formal assessment
- B. Regulatory overview
- C. Technical analysis
- D. Mutual evaluation

Answer: ([SHOW ANSWER](#))

In a mutual evaluation, a country must demonstrate to the FATF that it has an effective framework to protect its financial system from abuse. This process assesses both technical compliance with FATF Recommendations and the effectiveness of the country's AML/CFT measures.

NEW QUESTION: 88

How should national and sectoral risk assessments influence an organization's risk-based approach and internal risk assessment?

- A. They should be referenced and integrated appropriately into an organization's risk assessment to tailor enhanced due diligence (EDD) procedures and allocate resources effectively
- B. They provide general guidance but do not need to be directly considered because internal risk factors are more important
- C. They should only be referenced for high-risk clients as they are designed for worst-case scenarios
- D. They are primarily intended for regulators and should not influence organizational risk assessments

Answer: ([SHOW ANSWER](#))

FATF standards require organizations to adopt a risk-based approach (RBA) that is informed by both internal risk factors and national and sectoral risk assessments. These assessments provide critical insight into prevalent money laundering and terrorist financing threats within specific jurisdictions and industries.

Organizations should integrate relevant findings from these assessments into their internal risk assessments to ensure that policies, controls, and monitoring systems are aligned with identified risks. This enables institutions to tailor enhanced due diligence (EDD) measures and allocate compliance resources effectively.

Ignoring national or sectoral assessments would weaken the organization's ability to respond to known threats and would be inconsistent with regulatory expectations. These assessments are not limited to worst-case scenarios nor intended solely for regulators; they are a foundational input for private-sector AML programs.

NEW QUESTION: 89

Which of the following statements is true regarding tipping off?

- A. Tipping off is an obligation only applied to AFC professionals and bank staff because they are required to file a Suspicious Activity Report (SAR).
- B. Tipping off is a criminal act whereby confidential information about a financial crime investigation is disclosed in an unauthorized manner to a third party who may be the subject of the investigation or able to prejudice it.

C. Tipping off is not committed when detailed inquiries are made with a customer whose transactions have been flagged by a transaction monitoring system.

D. When an unusual transaction is detected, an AFC professional can instruct the relationship manager to communicate with the customer to decide whether a SAR should be filed.

Answer: (SHOW ANSWER)

"Tipping off" is a serious offense under AML/CFT legislation in many jurisdictions and is consistently addressed in FATF standards. It occurs when confidential information relating to a suspicious transaction, SAR, or ongoing investigation is disclosed without authorization to a person who is the subject of the report or whose knowledge could compromise the investigation. Such disclosures may alert criminals, allowing them to conceal evidence, move funds, or evade law enforcement. For this reason, tipping off is typically a criminal offense, not merely a breach of internal policy.

The prohibition applies broadly-not only to AFC professionals but to anyone with access to sensitive AML information. Making detailed or targeted inquiries with a customer after a transaction has been flagged can constitute tipping off if it reveals suspicion or investigative activity. Relationship managers must be carefully controlled and should not be instructed to probe customers in a way that signals suspicion.

Therefore, the correct statement is that tipping off is an unauthorized disclosure that can prejudice an investigation.

NEW QUESTION: 90

In a large US bank, an individual leads a team in charge of overseeing the governance and effectiveness of the bank's transaction monitoring approach. Which strategies should the team implement? (Select Two.)

A. Periodic and ad hoc cooperation with the legal team to appropriately investigate and monitor the transactions of subjects of subpoenas or government inquiries

B. Periodic review of client profiles to ensure that the most up-to-date information is on file for high-risk clients in line with the bank's internal policies and procedures

C. Periodic review of suspicious activity reports (SARs) filed with FinCEN to determine whether any should be withdrawn

D. Periodic review of the transaction monitoring scenarios and their productivity to ensure that appropriate AML typologies are reflected

Answer: (SHOW ANSWER)

Effective oversight of transaction monitoring includes:

Periodic review of client profiles to ensure up-to-date information for high-risk clients

(B): "Reviewing and updating customer profiles is essential to ensure that monitoring scenarios are based on current risk data." (CAMS 6th Edition, Transaction Monitoring and Customer Due Diligence) Periodic review of transaction monitoring scenarios and productivity to ensure appropriate AML typologies are reflected (D): "Firms should periodically review the parameters and output of transaction monitoring systems to ensure they continue to identify relevant ML/TF risks and typologies." (CAMS 6th Edition, Monitoring and Surveillance) Incorrect Options:

A: Cooperation with the legal team is important, but not a core strategy for monitoring governance.

C: SARs filed with FinCEN should not be withdrawn unless new evidence requires it; review should focus on process, not withdrawal.

References:

CAMS 6th Edition, Transaction Monitoring

FFIEC BSA/AML Manual, Transaction Monitoring Section

NEW QUESTION: 91

Tax evasion is:

- A. The practice of minimizing tax liability by exploiting loopholes or unintended interpretations of tax law
- B. A provision that reduces taxable income as an itemized or standard deduction
- C. A specialized accounting discipline focused on lawful tax planning
- D. The non-payment or under-payment of taxes, usually by deliberately making a false declaration or no declaration to tax authorities

Answer: (SHOW ANSWER)

Tax evasion is a criminal offense and is widely recognized as a predicate offense to money laundering under FATF standards and national AML laws.

It involves the deliberate non-payment or under-reporting of taxes, often through false declarations, concealment of income, or failure to file required tax returns. The key distinction is intentional deception of tax authorities.

In contrast, tax avoidance refers to lawful strategies used to minimize tax liability within the boundaries of the law. Deductions and tax planning activities are legal and do not constitute tax evasion.

Because tax evasion generates illicit proceeds, it is directly relevant to AML/CFT frameworks, and financial institutions must be alert to indicators of tax-related financial crime.

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 92

Key functions of the Financial Action Task Force (FATF) include: (Select Three.)

- A. Prosecuting non-cooperative jurisdictions
- B. Maintaining engagement with other international organizations and bodies

- C. Developing international standards to combat money laundering, terrorist financing, and proliferation financing
- D. Identifying and engaging with high-risk, non-cooperative jurisdictions with strategic deficiencies
- E. Suspending the membership of countries that perform poorly in mutual evaluations

Answer: ([SHOW ANSWER](#))

The Financial Action Task Force (FATF) is the global standard-setter for AML/CFT and counter-proliferation financing. Its mandate is focused on standard-setting, assessment, and international coordination, not enforcement or prosecution.

One of FATF's primary functions is developing international standards, known as the FATF Recommendations, which form the basis of national AML/CFT regimes worldwide.

FATF also identifies high-risk and non-cooperative jurisdictions with strategic AML/CFT deficiencies and works with them to address these weaknesses. Public identification encourages reform and enhances global financial integrity.

Additionally, FATF maintains strong engagement with international organizations, regional bodies, and the private sector to promote consistent implementation of standards.

FATF does not prosecute countries or suspend membership based on evaluation outcomes.

NEW QUESTION: 93

It is important for financial institutions (FIs) to be aware of anti-financial crime (AFC) and sanctions regulatory regimes in other jurisdictions in order to.

- A. ensure that sanctions regimes are applied selectively based on the regulatory standards of the countries where business activities occur, focusing primarily on aligned jurisdictions
- B. maintain compliance with the AFC and sanctions requirements of all countries where the FI operates or has business relationships and to avoid penalties for violations in foreign jurisdictions.
- C. ensure the FI can manage business relationships in jurisdictions with stricter or more lenient regulations than their home country, allowing for operational flexibility
- D. compensate for the limited applicability of AFC and sanctions regulations on cross-border transactions and their reduced relevance for domestic operations in other jurisdictions.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 94

In which of the following cases can a financial institution disclose a suspicious activity report (SAR)?

- A. A court order requests the bank to disclose the SAR subject to obtaining agreement from the legal team
- B. A customer asks about potential reporting to the local Financial Intelligence Unit (FIU)
- C. An external consultant inquires about the details of the SAR
- D. A third-country police directly inquires about the customer.

Answer: ([SHOW ANSWER](#))

A financial institution may disclose a SAR only under a valid court order and after ensuring legal review and compliance with jurisdictional requirements. In most jurisdictions, SARs are highly confidential, and unauthorized disclosure - known as "tipping off" - is prohibited.

NEW QUESTION: 95

An AML compliance officer receives an independent audit report with a number of findings.

An appropriate response to the report would include:

- A.** Assigning responsibility for reviewing the action plan to the board of directors
- B.** Reperforming the testing for the controls mentioned in the findings to confirm the results of the audit
- C.** Drafting detailed action plans for the audit team to execute to close the findings
- D.** Defining remedial actions based on the findings' root cause analysis

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

Which regulation is the cornerstone of AML/CFT legislation in the United States and requires financial institutions (FIs) to establish and maintain robust AML programs, including customer identification and due diligence procedures, as well as record-keeping and reporting of certain transactions to the Financial Crimes Enforcement Network (FinCEN)?

- A.** USA PATRIOT Act
- B.** Bank Secrecy Act (BSA)
- C.** Money Laundering Control Act (MLCA)
- D.** Markets in Crypto-Assets Regulation (MiCA)

Answer: ([SHOW ANSWER](#))

The Bank Secrecy Act (BSA) is the foundational Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) law in the United States. Enacted in 1970, the BSA requires financial institutions to establish and maintain effective AML programs designed to detect and prevent money laundering and terrorist financing.

Under the BSA and its implementing regulations, financial institutions must implement key controls such as Customer Identification Programs (CIP), customer due diligence (CDD), enhanced due diligence (EDD) for higher-risk customers, transaction monitoring, record-keeping, and the filing of Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) with FinCEN.

While the USA PATRIOT Act expanded AML obligations-particularly in relation to terrorist financing-it amended and strengthened the BSA rather than replacing it. The Money Laundering Control Act criminalized money laundering activities but does not establish the operational compliance framework. MiCA is an EU regulation and does not apply in the U.S.

Therefore, the BSA remains the cornerstone of U.S. AML/CFT compliance requirements.

NEW QUESTION: 97

Which of the following programs would most likely be considered part of an effective supervision regime for a regulator?

- A. Onsite and offsite reviews, cooperating on an international basis with access to a range of sanctions and outreach
- B. Onsite and offsite reviews, cooperating on an international and domestic basis with access to a range of sanctions and outreach
- C. Offsite reviews, cooperating on a domestic basis with access to a range of sanctions and outreach
- D. Onsite reviews, cooperating on an international and domestic basis with outreach and access to a range of sanctions

Answer: ([SHOW ANSWER](#))

An effective supervision regime includes both onsite and offsite reviews, cooperation on international and domestic levels, and access to a range of sanctions and outreach programs. This combination allows regulators to detect and address risks comprehensively while promoting compliance through engagement and enforcement.

NEW QUESTION: 98

Professional service providers-including lawyers, accountants, investment brokers, and other third parties-may abuse their positions to facilitate money laundering.

Which financial crime risks are associated with this type of abuse? (Select Three.)

- A. Opening an account to settle an estate on behalf of a client
- B. Establishing shell companies to enable money laundering activities, including placement or layering
- C. Opening third-party accounts for the primary purpose of masking the underlying client's identity
- D. Opening a trust account to facilitate a legitimate real estate transaction
- E. Directing or facilitating the laundering of illicit funds, including structuring transactions

Answer: ([SHOW ANSWER](#))

Professional service providers can be misused as enablers of money laundering when they abuse their trusted positions and expertise. FATF guidance highlights several risks linked to such abuse. The creation of shell companies is a common method used to obscure beneficial ownership and facilitate placement or layering of illicit funds. Similarly, opening third-party accounts to mask the true client identity directly undermines transparency and due diligence requirements.

Additionally, actively directing or facilitating the structuring or movement of illicit funds constitutes direct involvement in money laundering schemes and is a serious criminal offense.

By contrast, opening estate or trust accounts for legitimate, transparent purposes does not inherently pose a financial crime risk when proper due diligence is applied.

NEW QUESTION: 99

Criminals may misuse financial statements prepared by accountants to hide illicit assets.

Which of the following scenarios poses the greatest risk of financial statement manipulation by criminals?

- A.** A lack of professional body oversight or required use of accounting and auditing standards in the country of incorporation of the entity
- B.** Criminals posing as individuals seeking financial advice to place assets out of reach to avoid future liabilities
- C.** Incomplete records being provided during bookkeeping, making them difficult to audit
- D.** Accountants being used as intermediaries to introduce criminals to financial institutions

Answer: A ([LEAVE A REPLY](#))

A: The absence of professional oversight or accounting/auditing standards creates a high-risk environment for financial statement manipulation. Without external checks or mandated standards, criminals can more easily falsify statements to hide illicit assets.

"The lack of regulatory oversight and professional standards in accounting and auditing significantly increases the risk of manipulation and fraud in financial reporting."(CAMS 6th Edition, Professional Service Providers; FATF Guidance on the Risk-Based Approach for Accountants)

References:

CAMS 6th Edition, Professional Service Providers

FATF, Risk-Based Approach for Accountants

NEW QUESTION: 100

The Basel Committee on Banking Supervision (BCBS) is an international body consisting of senior representatives of central banks and banking regulatory authorities.

Which of the following statements accurately describe guidance provided by the BCBS? (Select Three.)

- A.** Since the Basel Committee has no enforcement authority, it relies on the commitment of its members to carry out its guidance
- B.** Basel guidance includes standards to be incorporated into local legal frameworks, guidelines for implementation, and best-practice guidance
- C.** The Basel Committee's Core Principles include guidance on customer identification and acceptance
- D.** Members of the BCBS must implement its standards or face suspension from membership
- E.** The Basel Committee is composed of the 28 largest banks in the world

Answer: ([SHOW ANSWER](#)**)**

The Basel Committee on Banking Supervision (BCBS) is a global standard-setting body that develops prudential banking standards and supervisory guidance, including key principles relevant to AML/CFT governance.

The BCBS does not have legal enforcement authority. Instead, it relies on the commitment of its member jurisdictions to implement its standards through national laws and supervisory practices. This cooperative model reflects the committee's role as a standard-setter rather than a regulator. Basel guidance includes international standards, implementation guidelines, and best practices designed to strengthen banking supervision and risk management frameworks globally. These materials are intended to be adopted and adapted within local legal and regulatory systems.

The Basel Core Principles for Effective Banking Supervision explicitly include guidance on customer identification, acceptance, and ongoing monitoring, aligning closely with AML/CFT expectations.

The committee is composed of central banks and supervisory authorities, not individual banks, and there are no formal penalties such as suspension for non-implementation.

NEW QUESTION: 101

Which of the following best describes the degree of cooperation between regulatory authorities, law enforcement agencies, and Financial Intelligence Units (FIUs) during money laundering investigations, including cross-border cases?

- A.** Regulatory authorities primarily work independently but share information when requested by international law enforcement agencies.
- B.** FIUs primarily handle reporting from financial institutions, while regulatory authorities and law enforcement agencies are limited to enforcing domestic AML laws without international cooperation.
- C.** Law enforcement agencies and FIUs only cooperate during domestic investigations, leaving cross-border investigations to international organizations like INTERPOL.
- D.** Regulatory authorities, law enforcement agencies, and FIUs share intelligence and coordinate efforts to streamline cross-border money laundering investigations, often through formal agreements.

Answer: ([SHOW ANSWER](#))

* D: "Cooperation and coordination between regulatory authorities, law enforcement agencies, and FIUs are essential for effective AML investigations, especially in cross-border cases. This is often accomplished through formal agreements, MOUs, and information-sharing mechanisms."(CAMS 6th Edition, International Cooperation in AML/CFT; FATF Recommendations 36-40) References:

CAMS 6th Edition, International Cooperation

FATF Recommendations 36-40

NEW QUESTION: 102

Which measures should be implemented to facilitate collaboration among different risk management functions to enhance an organization's anti-financial crime (AFC) program? (Select Three.)

- A.** Establish a robust framework for continuous threat intelligence sharing
- B.** Have senior management accountability for AFC failures
- C.** Establish a reward program among risk management functions to encourage proactive controls
- D.** Develop cross-functional training programs on AFC risks, management strategies, and related technologies
- E.** Develop common metrics and key performance indicators

Answer: ([SHOW ANSWER](#))

An effective anti-financial crime (AFC) program relies on strong collaboration across risk management functions, including AML, fraud, sanctions, cybersecurity, and operational risk. Regulatory guidance encourages integrated approaches to managing financial crime risk. A framework for continuous threat intelligence sharing allows different functions to exchange insights on emerging risks, typologies, and vulnerabilities, improving the organization's ability to detect and respond to threats holistically.

Cross-functional training programs help ensure that staff across risk functions understand AFC risks, regulatory expectations, and the tools used to manage them. This fosters consistency and breaks down silos within the organization.

Developing common metrics and key performance indicators (KPIs) aligns objectives across functions and enables management to assess program effectiveness consistently.

While senior management accountability is essential for governance, it does not directly facilitate collaboration among risk functions. Reward programs are not standard or recommended measures in regulatory guidance for enhancing AFC collaboration.

NEW QUESTION: 103

What should a financial institution (FI) do in response to a formal law enforcement request to produce documents?

- A.** Designate a person responsible for the internal investigation in preparation of documents for the request
- B.** Verify the officer's identification and ask for the law enforcement request to be served when the Chief Executive Officer is available to sign for it
- C.** Ask for an extension to review the FI's privacy policy and confidentiality policy before providing any information under the law enforcement request
- D.** Keep senior management informed at all times to strategically organize a defense to terminate the law enforcement request

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 104

Reference data screening includes the screening of which types of datasets? (Select Two.)

- A.** Types of payment messages
- B.** Customers
- C.** Third-party service providers
- D.** Customer spouses

Answer: ([SHOW ANSWER](#))

Reference data screening is a core element of AML/CFT programs and typically covers: Customers (B): "All customers must be screened against sanctions, PEP, and adverse media lists as part of onboarding and ongoing due diligence." (CAMS 6th Edition, Due Diligence and Screening) Third-party service providers (C): "Screening should extend to relevant third parties, such as agents and service providers, to prevent indirect exposure to sanctioned entities." (CAMS 6th Edition, Third-Party Screening; FATF Recommendations) Incorrect Options:

A: Types of payment messages are not screened; the entities/individuals are.

D: Customer spouses may be screened in some KYC processes but are not a standard dataset for reference screening.

References:

CAMS 6th Edition, Due Diligence and Screening

FATF Recommendations 10, 13, and 16

NEW QUESTION: 105

According to the Financial Action Task Force's (FATF's) "Guidance for a Risk-Based Approach Life Insurance Sector," which of the following are money laundering red flags relating to the involvement of a third party in a life insurance product? (Select Two.)

A. A customer engages an attorney to consult on the issuance of the policy.

B. A customer transfers the policy to another insurance company unaffiliated with the original policy issuer.

C. Payments are regularly received from third parties that have no apparent relationship with the policy holder.

D. A customer names an apparently unrelated third party as a beneficiary.

Answer: (SHOW ANSWER)

FATF and CAMS 6th Edition highlight certain third-party activities as red flags for money laundering in the life insurance sector:

Payments are regularly received from third parties that have no apparent relationship with the policy holder (C): "Red flags include payments made by third parties, especially where there is no apparent connection between the third party and the policy holder." (FATF, Risk-Based Approach for Life Insurance Sector, Section IV: Red Flags; CAMS 6th Edition, Customer Due Diligence for Life Insurance) A customer names an apparently unrelated third party as a beneficiary (D): "Another warning sign is when beneficiaries have no apparent relation to the policyholder." (FATF, Ibid; CAMS 6th Edition, Life Insurance ML/TF Red Flags) Incorrect Options:

A: Consulting an attorney is not, by itself, a red flag.

B: Policy transfer may warrant review but is not specifically a red flag for third-party involvement.

References:

CAMS 6th Edition, Life Insurance ML/TF Risks

FATF, Guidance for a Risk-Based Approach for the Life Insurance Sector (October 2018)

NEW QUESTION: 106

Which scenario indicates potential money laundering activity by a lawyer?

A. A lawyer's trust account receives a large-value wire transfer from a regulated insurance company and immediately transfers the same amount of funds received to the beneficiary's bank account located in a low-risk country.

B. A lawyer's trust account receives a large wire transfer deposit from a client that wanted to purchase a piece of property and then transfers the same amount to the property seller's lawyer's trust account.

- C.** A lawyer's trust account regularly receives wire transfers from unknown remitters from a higher risk country and immediately transfers the same amount of funds received to a known beneficiary's account in a low-risk country.
- D.** A lawyer located in a higher risk country deposits their firm's bank draft issued from their trust account to another lawyer's trust account located in a low-risk country for legal services rendered.

Answer: C ([LEAVE A REPLY](#))

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!
EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CAMS7 dumps with Test Engine here:
<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (**447 Q&As Dumps, 35%OFF**
Special Discount Code: freeexam)

NEW QUESTION: 107

While there are legitimate reasons for trust and company service providers (TCSPs) to appoint a nominee shareholder, which feature of a nominee shareholder presents the greatest financial crime risk?

- A.** Helping non-residents comply with local ownership laws
- B.** Simplifying administrative tasks associated with shareholding
- C.** Providing anonymity for the beneficial owner by keeping their identity hidden from the public register
- D.** Supporting company liquidity and ease of exit strategies

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 108

An AML compliance officer is drafting plans to address deficiencies identified in an independent audit.

Which approach is the best option?

- A.** Only commit to action plans that require no new investment to maximize shareholder value
- B.** Only commit to action plans that can be implemented and closed within the three-month management reporting cycle
- C.** Draft action plans in consultation with the jurisdiction's FIU to remain aligned with other similar companies
- D.** Draft action plans to address the root cause of the deficiencies, regardless of how long they will take to fully implement

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 109

A recruitment manager in the human resources department of a bank has shortlisted a candidate for the position of relationship manager in its private banking division. The compliance policy of the bank stipulates that proper background checks on new employees must be completed by the recruiting team to protect the bank against potential risks, including fraud and money laundering. Which resources would be most useful for identifying any potential negative information regarding the shortlisted candidate? (Select Three.)

- A. Criminal history searches
- B. Personal resume
- C. Personal references from close associates
- D. Past employment records
- E. Internet and public media searches

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 110

When selecting an anti-financial crime (AFC) tool for an organization, the most important factor to consider is whether the tool:

- A. integrates seamlessly with existing systems and processes.
- B. meets budget and cost requirements.
- C. automates all regulatory reporting requirements.
- D. replaces manual compliance training for employees.

Answer: ([SHOW ANSWER](#))

The most important factor when selecting an anti-financial crime tool is its ability to integrate seamlessly with existing systems and processes. Effective integration ensures data consistency, operational efficiency, and improved detection and response to financial crime risks.

NEW QUESTION: 111

Non-compliance with relevant anti-money laundering laws and regulations can result in: (Select Two.)

- A. delisting of public filing status.
- B. inclusion on the UN Consolidated List.
- C. civil and criminal penalties
- D. increased reputation risk.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 112

Which risk factors should a financial institution (FI) examine for a new corporate customer intending to open a new bank account? (Select Three.)

- A. The identity of senior managing officials and all individuals authorized to operate the account
- B. The employment profiles and information of all employees of the new customer
- C. All the financial institutions where the new customer currently banks or banked previously
- D. The type of business the corporate customer is engaged in

E. The country or location where the customer is from or conducts business

Answer: A,D,E ([LEAVE A REPLY](#))

NEW QUESTION: 113

Common risks and red flags associated with trade finance clients may include: (Choose four.)

- A. account activity that is not consistent with the purpose of the account
- B. bills of lading matching the description of goods, quantities, and values with transshipment details justified
- C. transaction structures that appear unnecessarily complex
- D. trade documents, such as invoices and letters of credit, that are not clearly worded or are in foreign languages
- E. invoices with prices that are much higher than market price
- F. fluctuations in the pricing of standard goods and services

Answer: ([SHOW ANSWER](#))

Trade finance red flags include account activity inconsistent with the account's stated purpose, unnecessarily complex transaction structures, poorly worded or foreign-language trade documents that may obscure details, and invoices with prices significantly above market value, which can indicate trade-based money laundering or fraud.

NEW QUESTION: 114

When considering purchasing AFC tools from a vendor to implement into the customer lifecycle, which of the following measures should be taken during the process? (Choose two.)

- A. Ensuring the tools are compatible and integration with current systems is possible
- B. Assessing whether internal staff members can provide training on the tools
- C. Assessing the cost of implementation and cost of maintaining the tools
- D. Basing business requirements on the features offered by the vendor's tools

Answer: ([SHOW ANSWER](#))

It is essential to ensure that anti-financial crime (AFC) tools are compatible and can be integrated with existing systems to avoid operational disruptions. Additionally, evaluating both implementation and ongoing maintenance costs is crucial for long-term sustainability and effective budget planning.

NEW QUESTION: 115

An internal audit team is reviewing the anti-financial crime (AFC) program of its firm. Which of the following attributes of the third line of defense would be most critical to ensure unbiased and effective oversight?

- A. Consistency of approach
- B. Periodic training of the function
- C. Qualification of the team
- D. Independent testing

Answer: ([SHOW ANSWER](#))

Independent testing is critical for the third line of defense to provide unbiased and effective oversight, ensuring that reviews and audits are objective and free from influence by the first or second lines of defense.

NEW QUESTION: 116

Which changes at a financial institution (FI) should trigger an enterprise-wide reassessment of its inherent AML risk exposure? (Select Three.)

- A. Mergers or acquisitions
- B. Use of new technologies for delivering existing products
- C. Restructuring of the FI's risk and compliance functions
- D. Changes in the individuals overseeing the FI's product lines and sales strategies
- E. Introduction of new products or services

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 117

The first line of defense is responsible for:

- A. collecting complete customer information.
- B. ongoing screening of customers.
- C. suspicious activity and sanctions reporting.
- D. evaluating the effectiveness of compliance controls.

Answer: A ([LEAVE A REPLY](#))

The First Line of Defense (1LoD) consists of customer-facing business units (e.g., relationship managers, front-office staff, and operational teams). Their primary responsibility in financial crime risk management is to implement AML/CFT controls as part of daily operations. This includes Collecting complete customer information.

The First Line of Defense is responsible for conducting Know Your Customer (KYC) and Customer Due Diligence (CDD) during onboarding and throughout the customer relationship. Ensuring that all relevant customer details (e.g., identity, business purpose, ownership structure) are accurately collected and documented is crucial for mitigating financial crime risks.

NEW QUESTION: 118

A company is rapidly expanding into several international markets, including jurisdictions considered high risk in terms of regulatory oversight. The board has requested the Money Laundering Reporting Officer (MLRO) to review and adjust the company's anti-financial crime (AFC) compliance framework to align with the evolving regulatory landscape and expansion strategy. During this process, the MLRO identifies vulnerabilities, particularly in markets with AML deficiencies, and updates the framework to mitigate these risks.

Which element of the AFC compliance program does this process describe?

- A. Governance arrangements
- B. Transaction monitoring
- C. Training and awareness

D. Risk assessment

Answer: ([SHOW ANSWER](#))

This scenario describes the risk assessment element of an anti-financial crime (AFC) compliance program.

FATF standards require organizations to regularly assess and reassess their money laundering and terrorist financing risks, particularly when there are material changes to business models, geographic exposure, or regulatory environments.

The MLRO's review of the company's expansion into high-risk jurisdictions and identification of vulnerabilities reflects a dynamic and forward-looking risk assessment process. Updating the compliance framework to address identified risks ensures that controls remain proportionate and effective.

Risk assessments form the foundation of the risk-based approach and directly inform decisions on enhanced due diligence, monitoring, governance, and resource allocation. This process is distinct from transaction monitoring, governance arrangements, or training activities, although those elements may be updated as a result of the risk assessment.

NEW QUESTION: 119

In the context of terrorist financing, which of the following are potential indicators of the abuse of non-profit organizations (NPOs)? (Choose two.)

- A. Involvement in community development and humanitarian aid projects
- B. Large and unaccounted cash donations from anonymous sources
- C. Operating in high-risk jurisdictions with limited oversight
- D. Frequent changes in leadership and mission statements
- E. Extensive transparency in financial reporting and governance practices

Answer: ([SHOW ANSWER](#))

Potential indicators of terrorist financing abuse in non-profit organizations include large, unaccounted cash donations from anonymous sources, which can disguise illicit funding, and operations in high-risk jurisdictions with limited oversight, where regulatory and monitoring frameworks may be weak.

NEW QUESTION: 120

An AML compliance officer for a large bank has recently received an internal audit report on the private banking unit. The report revealed that the unit staff were not following risk-based due diligence procedures, so that the unit was not operating effectively.

Which immediate actions should the AML compliance officer consider to address these findings?

(Select Two.) Management Should implement a quality assurance program in the private banking unit

- A. The legal department should conduct a review to assess potential legal consequences.
- B. The board should review and approve a revised AML policy to change customer due diligence requirements in private banking.
- C. Private bankers should receive training on AML procedures.
- D. All employees should receive refresher AML training.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 121

Perpetual KYC includes: (Choose two.)

- A. triggers identifying static data changes and data based on client's behaviors in real time.
- B. periodic refreshing at one-, three- and five-year cycles.
- C. ability to prioritize better based on client data rather than driven by schedules alone.
- D. classification of clients into categories of risk.

Answer: (SHOW ANSWER)

Perpetual KYC (pKYC) involves real-time monitoring of data triggers, such as static changes or behavioral anomalies, and prioritization based on client-specific data rather than fixed refresh schedules. This dynamic approach enhances risk management by responding more quickly to changes in client risk profiles.

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 122

Which statements regarding using network analysis tools to determine links to criminality are true? (Choose three.)

- A. When using network analysis data to fight money laundering and financial crime, data protection and privacy can be disregarded because fighting crime takes precedent
- B. Network analysis tools are an efficient means of generating relevant results because they only need a limited amount of data and computation power and artificial intelligence (AI) allows less-skilled people to quickly learn to use these systems
- C. When using artificial intelligence (AI) with network analysis tools, it must be ensured that the algorithms used are not biased towards social criteria, such as race, gender, or religion
- D. Network analysis allows for the identification of individuals or entities in a network by analyzing connections or links between them and can be used to study a wide range of systems, such as social or transportation networks
- E. Analyzing relationships between individuals in a social network allows for the identification of hierarchies, the detection of behaviors and geographical movements, or an understanding of how groups are organized

Answer: (SHOW ANSWER)

When using network analysis tools, it's important to avoid algorithmic bias toward social criteria to ensure fairness, analyze connections between individuals or entities to identify links and

structures, and study relationships within networks to uncover hierarchies, behaviors, movements, and group organization relevant to detecting criminal activity.

NEW QUESTION: 123

A compliance officer is reviewing an institutional banking prospect proposal for a new foreign entity that is a multinational business but headquartered in a country where most businesses are state-owned.

Which risks should be prioritized in the review? (Choose two.)

- A. Politically exposed persons (PEPs)
- B. Capital flight risk
- C. Anti-bribery and corruption risk
- D. Tax evasion

Answer: A,C ([LEAVE A REPLY](#))

The review should prioritize politically exposed persons (PEPs) risk, as state ownership increases the likelihood of political connections, and anti-bribery and corruption risk, since such environments may have higher exposure to corrupt practices and misuse of influence.

NEW QUESTION: 124

The Financial Action Task Force (FATF) routinely publishes a catalogue of jurisdictions requiring enhanced monitoring which is commonly called the:

- A. red notice
- B. white list
- C. grey list
- D. yellow notice

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 125

How can public-private partnerships (PPPs) foster collaboration in the fight against financial crime? (Choose two.)

- A. Developing a culture of compliance
- B. Improving governance in the public sector by requesting feedback from financial institutions
- C. Reducing transaction monitoring false positives for all financial institutions
- D. Improving the quality and quantity of data available for analysis by sharing information

Answer: ([SHOW ANSWER](#)**)**

Public-private partnerships help develop a culture of compliance across sectors and improve the quality and quantity of data through information sharing, enhancing the collective ability to detect and prevent financial crime.

NEW QUESTION: 126

To provide aid in investigating a cross-border money laundering case, a Financial Intelligence Unit (FIU) that is a member of the Egmont Group can:

- A.** assist law enforcement in another country with a material ongoing investigation.
- B.** directly contact other FIUs in another country and share information pertinent to the investigation.
- C.** deputize its law enforcement investigators to assist in a material ongoing investigation in another country
- D.** directly contact financial institutions in another country and share information pertinent to the investigation.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 127

Which of the below statements are supported by the Financial Action Task Force (FATF) 40 Recommendations adopted in 2012? (Select Two.)

- A.** Nations should work towards implementing targeted financial sanctions in alignment with the UN Security Council.
- B.** Customer privacy regulations should guide the development of due diligence and other money laundering and terrorist financing preventive measures.
- C.** Nations should take measures to ensure there is transparency to the beneficial ownership of legal persons.
- D.** Governments must work toward developing identical administrative and operational frameworks for investigating and prosecuting crime.
- E.** Nations should establish frameworks that take a risk-based approach to prevent and mitigate money laundering and terrorist financing.
- F.** Regulators should direct Financial Institutions to establish appropriate frameworks to avoid banking higher risk customers.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 128

The UN Security Council's primary role in imposing sanctions is that it has the authority to:

- A.** impose sanctions to maintain or restore international peace and security
- B.** impose sanctions on countries that lack AML/CFT controls.
- C.** conduct research on and analyze the impacts of sanctions to improve the effectiveness of sanctions regimes.
- D.** impose sanctions on economic targets to maintain or restore financial stability within a country.

Answer: ([SHOW ANSWER](#))

The UN Security Council has the authority to impose sanctions specifically to maintain or restore international peace and security.

NEW QUESTION: 129

Which of the following is a key consideration for a global organization when managing AML and sanctions compliance across multiple jurisdictions?

- A.** Ensuring sanctions compliance by relying solely on international bodies like the UN because there is no requirement to adhere to local laws
- B.** Ensuring group policies and procedures prioritize adherence to US regulations because they are the most influential worldwide
- C.** Applying global AFC and sanctions policies to ensure consistency without the need to adapt to local regulations
- D.** Ensuring group policies cater to compliance with each country's specific AML and sanctions regulations

Answer: (SHOW ANSWER)

Global organizations must ensure their policies and procedures comply with local laws and regulations in each country where they operate, even when maintaining group-wide consistency. Relying solely on international or U.S. standards does not ensure compliance with all local requirements, which may be more stringent or specific.

"A global group-wide program should ensure adherence to local AML and sanctions laws and regulations in every jurisdiction in which it operates. Local adaptation of policies is essential to address jurisdiction-specific risks and legal requirements." (CAMS 6th Edition, International AML/CFT Standards; FATF Recommendations 18, 35; EU & US Sanctions Regulations)

References:

CAMS 6th Edition, Compliance Across Jurisdictions

FATF Recommendation 18: Internal Controls and Foreign Branches

Basel Committee on Banking Supervision (BCBS) Guidance

NEW QUESTION: 130

A recruitment manager in the human resources department of a bank has shortlisted a candidate for the position of relationship manager in its private banking division.

The bank's compliance policy requires proper background checks to protect against fraud and money laundering risks.

Which resources would be most useful for identifying potential negative information regarding the shortlisted candidate? (Select Three.)

- A.** Past employment records.
- B.** Personal references from close associates.
- C.** Personal resume.
- D.** Internet and public media searches.
- E.** Criminal history searches.

Answer: A,D,E (LEAVE A REPLY)

Financial institutions must conduct thorough background checks on employees in sensitive roles (e.g., private banking) to mitigate fraud, insider trading, and money laundering risks.

Option A (Correct): Past employment records help verify work history and identify any red flags related to prior financial misconduct.

Option D (Correct): Internet and media searches reveal any negative press, regulatory issues, or connections to illicit activity.

Option E (Correct):Criminal history searches help screen for prior convictions related to financial crimes.

Why Other Options Are Incorrect:

Option B (Incorrect):Personal references are less reliable and may not uncover objective risk factors.

Option C (Incorrect):A resume is self-reported and should be verified using independent sources.

Best Practices for Employee Background Screening:

Conduct enhanced due diligence for high-risk roles (e.g., private bankers, compliance officers).

Use reliable background screening tools and legal databases.

Verify employment history and check against regulatory blacklists.

Reference:

FATF Recommendation 18 (Internal Controls & Employee Screening)

Wolfsberg Group Guidance on AML Employee Background Checks

6th EU AML Directive (6AMLD) on Employee Due Diligence

NEW QUESTION: 131

Which factors should be prioritized when choosing an anti-financial crime (AFC) tool for an organization? (Select Two.)

- A. Real-time data analysis capabilities as part of a broader strategy
- B. Preference for the lowest-cost solution
- C. Complete elimination of manual processes
- D. Compatibility with existing IT infrastructure
- E. Scalability to handle increasing transaction volumes

Answer: ([SHOW ANSWER](#))

When selecting an anti-financial crime (AFC) tool, regulators and industry best practices emphasize effectiveness, sustainability, and integration over cost or automation alone.

Compatibility with existing IT infrastructure is critical to ensure seamless data integration, system stability, and governance. Poor integration can lead to data gaps, operational risk, and ineffective monitoring.

Scalability is equally important, as transaction volumes, customer bases, and regulatory requirements grow over time. An AFC tool must be able to handle increased workloads without degradation in performance or effectiveness.

While real-time analytics may be beneficial, they must align with the organization's overall risk strategy and system capabilities. Lowest cost and full elimination of manual processes are not regulatory priorities; human oversight remains essential in AML/CFT programs.

NEW QUESTION: 132

A key advantage of privacy enhancing technologies (PETs) in anti-money laundering is that they offer:

- A. simultaneous encryption and decryption for underlying data.
- B. full access to underlying data with full and uninterrupted calculations made on the data.

- C. secure processing of data while it remains encrypted.
- D. transfer, decryption and storage of data by the data processor.

Answer: C ([LEAVE A REPLY](#))

A key advantage of privacy enhancing technologies (PETs) in anti-money laundering is their ability to securely process data while it remains encrypted. This enables data analysis and collaboration without exposing sensitive information, helping to maintain privacy while still supporting financial crime detection.

NEW QUESTION: 133

Customer segmentation is important for effective transaction monitoring because:

- A. All customers transact in the same way, allowing patterns to be easily spotted
- B. Customer behavior can be compared and analyzed most effectively among similar peer groups
- C. It allows a broad range of customer types to be compared in one large group
- D. It is recommended by regulators solely to prevent sanctions risk

Answer: ([SHOW ANSWER](#)**)**

Customer segmentation is a foundational element of effective transaction monitoring and is strongly aligned with the risk-based approach promoted by FATF and national regulators.

Customers differ significantly in their transaction behavior depending on factors such as customer type, industry, geography, products used, and transaction volumes. By grouping customers into similar peer segments, institutions can more accurately establish expected behavior and identify anomalies that may indicate suspicious activity.

Comparing customers across a single large population would mask meaningful deviations and generate excessive false positives or missed risks. Segmentation improves alert quality, efficiency, and investigative focus.

Customer segmentation is not limited to sanctions compliance; it is a core AML transaction monitoring practice used to detect money laundering, terrorist financing, and other financial crimes.

NEW QUESTION: 134

While there are legitimate reasons for trust and company service providers (TCSPs) to appoint a nominee shareholder, which feature of a nominee shareholder presents the greatest financial crime risk?

- A. Supporting company liquidity and ease of exit strategies
- B. Providing anonymity for the beneficial owner by keeping their identity hidden from the public register
- C. Simplifying administrative tasks associated with shareholding
- D. Helping non-residents comply with local ownership laws

Answer: ([SHOW ANSWER](#)**)**

Nominee shareholders may be used for legitimate commercial reasons; however, FATF guidance identifies nominee arrangements as a significant money laundering risk when they obscure beneficial ownership.

The greatest risk arises when nominee shareholders provide anonymity to the true beneficial owner, preventing transparency in public registers and complicating due diligence. Criminals may exploit this opacity to conceal ownership, evade sanctions, launder illicit proceeds, or avoid tax and regulatory scrutiny.

The ability to hide ownership undermines one of the core objectives of AML/CFT frameworks: identifying and verifying beneficial owners. As a result, regulators require enhanced due diligence and clear documentation when nominee shareholders are involved.

Other features-such as administrative efficiency, compliance with local laws, or ease of share transfer-do not inherently increase financial crime risk when transparency and disclosure requirements are met.

NEW QUESTION: 135

A National Risk Assessment (NRA) can impact a financial institution's (FI's) risk-based approach to anti- money laundering and terrorism financing by:

- A. dictating what predicate offences must be considered in the FI's risk assessment.
- B. providing guidance on the types of customers and transactions that pose the highest risk.
- C. defining exactly what policies and procedures must be implemented.
- D. determining the maximum fines that can be imposed for AML violations.

Answer: (SHOW ANSWER)

A National Risk Assessment (NRA) provides valuable guidance on which customers, products, services, and transactions pose the highest risk for money laundering and terrorist financing, enabling financial institutions to tailor their risk-based approach and allocate resources more effectively.

NEW QUESTION: 136

A financial crimes risk appetite statement describes:

- A. how an organization determines its key risk and performance indicators.
- B. the level and type of risk the organization is willing to take to meet its objectives
- C. the purpose of an organization's financial crimes compliance program.
- D. how an organization defines Its risk-based approach.

Answer: (SHOW ANSWER)

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 137

A bank has joined a public-private partnership (PPP) to work with law enforcement and regulators on combating financial crime. However, the bank's data protection officer is concerned about sharing sensitive customer data, and the compliance officer is worried about potential delays in receiving useful information from the government.

Which of the following best describes a benefit of PPPs in fighting financial crime?

- A.** PPPs maximize the efficiency of the bank's compliance program by providing real-time intelligence from law enforcement.
- B.** PPPs improve financial crime detection and prevention by sharing intelligence between banks and law enforcement.
- C.** PPPs allow banks to manage their own suspicious activity report (SAR) filing process without the need to involve the Financial Intelligence Unit (FIU).
- D.** PPPs help banks reduce compliance costs by automating information sharing.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 138

A financial institution is designing an enterprise-wide risk assessment (EWRA).

According to the guidance issued by the Wolfsberg Group regarding a risk-based approach to identifying and managing money laundering risks, an effective approach should:

- A.** Use a framework provided by a third-party vendor and used by other FIs in the jurisdiction.
- B.** Include appropriate measures and controls to mitigate money laundering risks stemming from higher- risk customers, products, and geographies.
- C.** Focus on the inherent risk in the FI's product and service offerings and the controls to mitigate potential money laundering risks.
- D.** Focus on understanding the risks presented by new clients within the assessment period, and the controls to mitigate associated money laundering risks.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 139

Which activities are part of adverse media screening for negative news and reputational risks? (Select Three.)

- A.** Analyzing customer sentiment through feedback and surveys
- B.** Identifying individuals or entities linked to criminal activities or sanctions
- C.** Periodically monitoring regulatory updates and enforcement actions for associated entities
- D.** Scanning publicly available news articles and regulatory alerts
- E.** Monitoring changes in credit scores of individuals or entities

Answer: ([SHOW ANSWER](#))

Adverse media screening seeks to identify reputational or financial crime risk by:

- * B: Identifying links to criminal activity or sanctions.
- * C: Monitoring regulatory actions and updates for risk associations.
- * D: Regularly scanning news and public records for negative information.

"Adverse media screening involves collecting and reviewing publicly available information, news, and regulatory actions to detect links to criminal activity or reputational risks." (CAMS 6th Edition, Adverse Media Screening; FATF Guidance) Incorrect:

* A and E: Customer sentiment and credit scores are not core to adverse media screening.

References:

CAMS 6th Edition, Customer Due Diligence and Screening

FATF Guidance on Customer Due Diligence

NEW QUESTION: 140

In order to prevent financial crime risk, the implemented policies, controls, and procedures must:

- A.** Be proportionate to the size and nature of the firm, approved by senior management, and regularly reviewed
- B.** Be created, approved, and owned only by the First Line of Defense and reviewed annually
- C.** Be completed by the business and validated by an external firm
- D.** Include sophisticated and automated controls using the newest available technologies

Answer: ([SHOW ANSWER](#))

Effective AML/CFT policies, controls, and procedures must be risk-based, proportionate, and well-governed, as emphasized by FATF and national regulators. Proportionality ensures that controls are appropriate to the firm's size, complexity, products, services, and risk exposure. Senior management approval is essential to establish accountability and tone from the top. Regular review ensures policies remain effective as risks, regulations, and business models evolve.

AML responsibility is shared across the three lines of defense, not owned solely by the business. External validation may support assurance but does not replace internal accountability. While technology can enhance controls, regulators do not mandate the use of advanced or cutting-edge solutions; effectiveness and governance are more important than sophistication.

NEW QUESTION: 141

A client advisor at a bank contacts a member of the compliance team for guidance on how to proceed with a client who wants to transfer US\$250,000 from the sale of cryptoassets into their savings account at the bank.

What guidance should the compliance team provide?

- A.** Advise further clarification is necessary, including which coins or tokens were sold and whether the crypto exchange conducts due diligence on its clients
- B.** Advise that the transaction should be stopped because cryptoassets in general are not regulated and by definition pose an unacceptable AML risk for the bank
- C.** Confirm to the advisor that the customer can proceed with the transaction if the client's KYC is up to date and a search on a public blockchain explorer does not provide any adverse media hits
- D.** Confirm to the advisor that the customer can proceed with the transaction because clients are already correctly onboarded KYC is complete and the source of funds is transparent

Answer: ([SHOW ANSWER](#))

The compliance team should request further clarification to assess the AML risk appropriately. This includes understanding which cryptoassets were sold and whether the exchange used applies adequate due diligence. These details help determine the legitimacy of the source of funds and ensure compliance with AML requirements.

NEW QUESTION: 142

A global financial institution is conducting a comprehensive review of its due diligence processes to strengthen its defenses against financial crime. Recent incidents have highlighted vulnerabilities related to employee misconduct, including unauthorized transactions and sharing of sensitive customer information.

Additionally, the FI has faced issues with third-party vendors who failed to meet compliance standards, leading to increased regulatory scrutiny.

Which of the following measures would be most effective in addressing the bank's due diligence needs for employees, vendors, and third parties to mitigate insider threats and ensure compliance with AML regulations?

- A.** Relying on self-reported compliance certifications from vendors and employees to confirm adherence to AML standards on a periodic basis
- B.** Establishing a surveillance program for employees, vendors, and third parties, including periodic risk assessments, access controls, and regular reviews of their compliance with AML policies
- C.** Implementing background checks for employees and vendors prior to onboarding or the start of engagement to identify any red flags
- D.** Limiting the number of vendors and third parties in high-risk jurisdictions in order to reduce exposure to compliance risks

Answer: ([SHOW ANSWER](#))

Establishing a surveillance program with periodic risk assessments, access controls, and regular compliance reviews for employees, vendors, and third parties is the most effective way to mitigate insider threats and ensure ongoing adherence to AML regulations. This proactive approach continuously monitors risk rather than relying solely on initial checks or self-certifications.

NEW QUESTION: 143

Which financial crime risks are inherent to e-commerce platforms? (Select Four.)

- A.** E-commerce platforms exploited to move criminal proceeds
- B.** Use of stolen bank cards for online purchases
- C.** E-commerce platforms susceptible to fraud schemes
- D.** E-commerce platforms used as a front for illicit transactions
- E.** E-commerce platforms encouraging unregulated peer-to-peer lending
- F.** Use of foreign currency to mask criminal proceeds

Answer: ([SHOW ANSWER](#))

* A, B, C, D are all identified by CAMS 6th Edition and FATF as primary financial crime risks for e-commerce platforms:

* A: Platforms can be exploited to launder money by processing the movement of criminal proceeds under the guise of legitimate sales.

* B: Use of stolen credit/debit cards for online purchases is a common fraud and ML technique.

* C: Fraud schemes (such as chargebacks or fake listings) are widespread on e-commerce platforms.

* D: E-commerce platforms can serve as fronts for illicit goods or services, masking the true nature of transactions.

* E and F are not commonly cited as principal inherent risks in AML/CTF guidance.

References:

CAMS 6th Edition, E-commerce ML/TF Risks

FATF, "Money Laundering Risks Arising from E-commerce Activities"

NEW QUESTION: 144

When a multinational organization develops its anti-financial crime (AFC) program, what is the most important consideration for ensuring compliance across different jurisdictions?

A. Ensuring sanctions comply on international bodies like the UN because there is no requirement to adhere to local laws.

B. Ensuring group policies and procedures prioritize adherence to US regulations because they are the most influential worldwide.

C. Applying global AFC and sanctions policies to ensure consistency without the need to adapt to local regulations.

D. Ensuring group policies cater to compliance with each country's specific AML and sanctions regulations.

Answer: ([SHOW ANSWER](#))

A global organization must ensure its group policies accommodate compliance with each country's specific AML and sanctions regulations to effectively manage risks across multiple jurisdictions.

NEW QUESTION: 145

Which of the following scenarios exhibit classic indicators of suspicious transactions? (Select Two.)

A. A business owner mortgages his home with a financial institution that was recently fined for AML violations

B. A customer regularly invests in equity funds using her spouse's bank account where she is a second account holder

C. An individual who is the secretary to a government official frequently accesses the bank's safe deposit vault to withdraw cash

D. An individual regularly imports sophisticated electronic items for civil use and pays all applicable customs duties

E. An individual wants to execute wire transfers to a person in a FATF grey-listed jurisdiction and asks a close friend to send the money on his behalf, citing financial difficulties

Answer: ([SHOW ANSWER](#))

Classic indicators of suspicious activity often involve use of proxies, unusual cash access, or attempts to avoid scrutiny, as highlighted in FATF and FIU guidance.

Frequent access to a safe deposit vault to withdraw cash by a person closely associated with a government official raises heightened concern. Such behavior may indicate attempts to conceal illicit funds, particularly given the potential exposure to corruption risk associated with politically exposed persons (PEPs) and their close associates.

Similarly, requesting a third party to execute wire transfers on one's behalf to a FATF grey-listed jurisdiction is a well-recognized red flag. This behavior suggests an attempt to evade transaction monitoring, sanctions screening, or enhanced due diligence requirements by distancing oneself from the transaction.

The remaining scenarios describe activities that are either legitimate or explainable with proper documentation and transparency. Merely dealing with an institution previously fined for AML violations or conducting legitimate trade with customs compliance does not, on its own, constitute suspicious activity.

NEW QUESTION: 146

Beyond the physical and mental harm caused to individuals, which of the following problems can be linked to significant costs from unregulated online gambling and gaming?

- A.** Economic and societal
- B.** Political and regulatory
- C.** Governance and compliance
- D.** Sectoral and jurisdictional

Answer: ([SHOW ANSWER](#))

Unregulated online gambling and gaming can lead to significant economic and societal costs, including increased crime, financial distress, addiction, and strain on public health and social services. These impacts extend beyond individual harm and affect communities and national economies.

NEW QUESTION: 147

Risks associated with real estate transactions include (Select Two.)

- A.** cross-border purchases.
- B.** purchases in the name of a natural person.
- C.** paying true market price for a property.
- D.** non-financed purchases.

Answer: ([SHOW ANSWER](#))

Real estate transactions are vulnerable to ML/TF risks, particularly when there is limited transparency or unusual payment methods:

Cross-border purchases (A): "Purchases by foreign buyers, especially from high-risk jurisdictions, are a red flag for money laundering in the real estate sector." (CAMS 6th Edition, Real Estate Money Laundering Risks; FATF, Money Laundering and Terrorist Financing through the Real Estate Sector, 2007) Non-financed purchases (D): "Non-financed (all-cash) purchases can indicate the introduction of illicit funds into the financial system, bypassing the controls of mortgage lenders." (CAMS 6th Edition, Real Estate ML/TF Risks)

Incorrect Options:

B: Purchasing in the name of a natural person is standard and not inherently risky.

C: Paying the true market price does not raise ML/TF risk.

References:

CAMS 6th Edition, Chapter: ML/TF Risks in Real Estate

FATF, Money Laundering and Terrorist Financing through the Real Estate Sector (2007)

NEW QUESTION: 148

Risks associated with real estate transactions include: (Choose two.)

- A. cross-border purchases
- B. purchases in the name of a natural person
- C. paying true market price for a property
- D. non-financed purchases

Answer: ([SHOW ANSWER](#))

Cross-border purchases increase complexity and risk due to differing regulations and potential anonymity.

Non-financed purchases, especially in cash, can facilitate money laundering by avoiding traditional financial scrutiny.

NEW QUESTION: 149

The primary roles of a Country's Financial Intelligence Unit (FIU) include: (Select Two.)

- A. conducting examinations of financial institutions to ensure compliance with anti-money laundering regulations.
- B. collaborating with law enforcement agencies, financial institutions, and other stakeholders to detect and prevent illicit financial activities.
- C. engaging in providing financial services, including banking and investment activities, to the public and private sectors
- D. enacting legislation regarding the operations of financial institutions.
- E. facilitating the exchange of information between the public and private sectors.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 150

A large international financial institution (FI) operates in both the United States and the European Union. A cross-border transaction involving a high-net-worth client with dual U.S. and French citizenship raises concerns due to a third-party intermediary in a high-risk jurisdiction. Given that the transaction falls under the U.S. Bank Secrecy Act (BSA) and OFAC requirements, as well as the EU's 6th Anti-Money Laundering Directive (6AMLD) and European Banking Authority (EBA) regulations, what is the best approach for the compliance team to ensure compliance?

- A. Follow EU regulations only, as the beneficiary is based in France
- B. Implement a dual-compliance approach satisfying both U.S. and EU AML regulations
- C. Defer to the most stringent regulatory regime to streamline compliance
- D. Follow U.S. regulations only, as the transaction originates in the United States

Answer: ([SHOW ANSWER](#))

For multinational financial institutions, regulatory expectations are clear: institutions must comply with all applicable laws and regulations in each jurisdiction where they operate or where a transaction has regulatory touchpoints.

In this case, the transaction is subject to both U.S. and EU AML/CFT frameworks, including BSA reporting obligations, OFAC sanctions screening, 6AMLD requirements, and EBA supervisory expectations.

Selecting only one regulatory regime would expose the institution to compliance failures and enforcement risk.

A dual-compliance approach ensures that reporting, sanctions screening, customer due diligence, and record-keeping obligations are met in both jurisdictions. This approach aligns with FATF principles on cross-border compliance and consolidated supervision.

Deferring to the "most stringent" regime is not sufficient, as different rules may apply to different aspects of the transaction. Therefore, simultaneous compliance is required.

NEW QUESTION: 151

Artificial intelligence (AI) and machine learning (ML) procedures help in applying a risk-based approach in AML compliance through: (Select Three.)

- A. Automatically generating Suspicious Activity Reports (SARs) without the need for human review
- B. Advanced customer risk assessments that synthesize client background information with additional data
- C. Identification of links among apparently unrelated clients who have established complex networks for money laundering
- D. Automatically adapting risk thresholds for customers without any human intervention
- E. Detection of complex money laundering patterns in transactions

Answer: ([SHOW ANSWER](#))

Artificial intelligence and machine learning technologies support the risk-based approach (RBA) to AML compliance by enhancing an institution's ability to identify, assess, and prioritize financial crime risks.

Regulatory guidance emphasizes that these technologies should augment-not replace-human judgment.

One key benefit is advanced customer risk assessment. AI and ML can synthesize large volumes of customer data, including background information, transaction behavior, and external risk indicators, allowing institutions to develop more accurate and dynamic risk profiles.

AI and ML also enable the identification of complex networks among seemingly unrelated clients. Through network analytics and pattern recognition, these tools can uncover hidden relationships used in layering and structuring activities.

Additionally, AI-driven systems excel at detecting complex money laundering patterns within transaction data that may not trigger traditional rule-based alerts, improving effectiveness and efficiency.

Automatically generating SARs or adapting thresholds without human oversight is inconsistent with regulatory expectations. Human review and governance remain essential components of AML compliance.

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 152

When deciding on the fuzzy matching threshold for sanctions screening, consideration should be given to:

- A.** the operational burden of dealing with potential matches.
- B.** the value of fines for non-compliance.
- C.** the experience of the team dealing with potential matches.
- D.** whether the data to be screened is reliable and verified.

Answer: ([**SHOW ANSWER**](#)**)**

When setting a fuzzy matching threshold for sanctions screening, it is crucial to consider the reliability and accuracy of the data being screened. High-quality, verified data supports more effective matching and reduces both false positives and the risk of missing true matches.

NEW QUESTION: 153

What is the first step in designing an effective controls framework using a risk-based approach?

- A.** Establishing risk controls
- B.** Assessing risk controls
- C.** Ongoing risk monitoring
- D.** Conducting a risk assessment

Answer: ([**SHOW ANSWER**](#)**)**

The first step in designing an effective controls framework using a risk-based approach is conducting a risk assessment. This identifies and evaluates inherent risks, providing the basis for determining which controls are necessary and how they should be prioritized.

NEW QUESTION: 154

The United Nations Security Council's sanctions are intended to be:

- A. Encompassing and broad, including the use of force if necessary
- B. Designed to maintain and restore international peace and security
- C. Indefinite to produce economic benefit for a group of states
- D. Punitive to influence foreign governments to change their behavior

Answer: ([SHOW ANSWER](#))

United Nations Security Council (UNSC) sanctions are a key international tool established under Chapter VII of the UN Charter. Their primary purpose is to maintain or restore international peace and security, not to punish states or provide economic advantage.

Sanctions may include asset freezes, travel bans, arms embargoes, or targeted measures against individuals and entities. These measures are designed to influence behavior, prevent escalation of conflict, and support diplomatic solutions.

The use of force is separate from sanctions and requires explicit authorization. Sanctions are not intended to be indefinite and are regularly reviewed and adjusted based on effectiveness and humanitarian considerations.

While sanctions may exert pressure on governments or actors, they are not intended as punitive measures but as preventive and corrective tools aligned with international law.

NEW QUESTION: 155

An EU Trust and Company Service Provider analyst notices some unusual activity while looking through a customer's financial statements and detailed general ledger. The customer is in the business of importing and exporting machineries.

Which transaction indicator warrants further escalation to the compliance officer?

- A. The payment of consultancy fees to unrelated companies and service providers established in a foreign jurisdiction
- B. The payment of virtual offices services overseas
- C. The payment of company secretarial retainer fees to a foreign company in a tax-efficient jurisdiction
- D. Inter-company loans from the holding company to the subsidiary company to finance the shipment of machinery

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 156

A team overseeing the governance and effectiveness of a bank's transaction monitoring approach should implement which strategies? (Select Two.)

- A.** Periodic review of suspicious activity reports (SARs) filed with FinCEN to determine whether any should be withdrawn.
- B.** Periodic and ad hoc cooperation with the legal team to appropriately investigate and monitor the transactions of subjects of subpoenas or government inquiries.
- C.** Periodic review of client profiles to ensure that the most up-to-date information is on file for high-risk clients in line with the bank's internal policies and procedures.
- D.** Periodic review of the transaction monitoring scenarios and their productivity to ensure that appropriate AML typologies are reflected.

Answer: B,D (LEAVE A REPLY)

Transaction monitoring governance involves ensuring that AML detection systems are effective, aligned with regulatory standards, and capable of identifying evolving threats.

Option B (Correct): Legal cooperation is essential for responding to subpoenas and law enforcement inquiries.

Option D (Correct): Regularly updating transaction monitoring scenarios ensures that the system adapts to emerging financial crime trends.

Why Other Options Are Incorrect:

Option A (Incorrect): SARs cannot be withdrawn unless an error was made—once filed, SARs remain confidential and must be retained.

Option C (Incorrect): Client profile updates are a CDD/KYC function, not directly related to transaction monitoring governance.

Best Practices for Transaction Monitoring Governance:

Regularly review system effectiveness through validation tests.

Collaborate with legal and compliance teams for risk mitigation.

Use AI and data analytics to refine detection accuracy.

Reference:

FATF Recommendation 10 (Customer Due Diligence & Ongoing Monitoring)

Wolfsberg Group Guidance on Transaction Monitoring Effectiveness

Basel Committee's Guidelines on AML Technology and Data Analytics

NEW QUESTION: 157

An agent of a wealthy individual residing in Country A, which is on the EU list of high-risk third jurisdictions, approaches a notary in Country B, which is in the EU. The agent wants to complete a disposal of assets recently acquired at auction by the wealthy individual through an offshore company. The agent also has a power of attorney to act on behalf of the offshore company issued by a respectable law firm from Country C, which is also in the EU. The agent asks the notary to proceed with the disposal as quickly as possible without paying any specific attention to related costs or taxes to be paid as a result of this transaction. The notary notices the intended transfer price is significantly lower than the one recorded at auction, but the agent does not want to discuss this matter and claims that it is not covered by the power of attorney.

Which red flags should the notary consider? (Select Two)

- A.** The agent requested a disposal of assets at a lower price than recently acquired.

- B.** The assets acquired through an auction were put in the name of an offshore company
- C.** The agent acted on behalf of an individual residing in a country which is on the EU's list of high-risk jurisdictions
- D.** The power of attorney was issued by a law firm in a different EU country from where the transaction took place.

Answer: ([SHOW ANSWER](#))

A: Selling assets at a significant loss, especially shortly after purchase, is a classic red flag for asset laundering and value manipulation, which can be used to disguise the true nature of proceeds.

C: Transactions involving individuals from high-risk jurisdictions, as identified by the EU and FATF, warrant heightened scrutiny due to increased ML/TF risk. (CAMS 6th Edition, Red Flags for Complex Asset Transactions; EU List of High-Risk Third Countries) B and D may contribute to complexity but are not the primary red flags in this scenario.

References:

CAMS 6th Edition, Red Flags in Notarial and Legal Transactions

EU AML Directives and High-Risk Country Lists

NEW QUESTION: 158

A national risk assessment (NRA) can impact the risk-based approach (RBA) within an organization's anti- financial crime (AFC) compliance program by: (Choose two.)

- A.** helping to identify high-risk sectors that require enhanced due diligence (EDO),
- B.** eliminating the need for sectoral risk assessments within the organization
- C.** guiding the allocation of resources for mitigating financial crime risks
- D.** requiring all organizations to apply standardized measures
- E.** automatically reducing the organization's responsibility for conducting its own risk assessment

Answer: ([SHOW ANSWER](#))

A national risk assessment can identify high-risk sectors requiring enhanced due diligence and guide resource allocation to mitigate financial crime risks effectively, helping organizations align their risk-based approach with national priorities and threats.

NEW QUESTION: 159

Which activities would be considered money laundering red flags when reviewing the business operations of a money services business (MSB)? (Select Two.)

- A.** A customer being hesitant to provide beneficiary name or address information when sending international wire transfers
- B.** Cash-intensive businesses, such as convenience stores or restaurants, making large cash deposits
- C.** A customer exchanging foreign currency from a higher-risk jurisdiction for domestic currency under the reporting threshold
- D.** A customer using multiple accounts under different names to conduct transactions

E. A customer completing frequent small-dollar international money transfers to their native country

Answer: ([SHOW ANSWER](#))

When reviewing business operations of a Money Services Business (MSB), it is critical to identify behaviors that indicate potential money laundering activity. The CAMS Study Guide - 6th Edition outlines several red flags commonly associated with MSBs.

Option A is correct:

A customer being hesitant to provide beneficiary information, such as the name or address, is a red flag. It may indicate attempts to hide the true purpose or recipient of the funds and could suggest structuring or layering activity.

Option D is correct:

A customer using multiple accounts under different names to conduct transactions is a strong red flag. This could indicate efforts to obscure ownership, avoid detection, or conduct suspicious structuring behavior to stay below reporting thresholds.

Option B is incorrect:

While large cash deposits from cash-intensive businesses may require further review, they are not inherently suspicious unless inconsistent with the nature of the business or transaction volume.

Option C is incorrect:

Currency exchanges under the reporting threshold, even from high-risk jurisdictions, are not in themselves red flags unless they show a pattern of structuring or are part of larger suspicious behavior.

Option E is incorrect:

Frequent small-dollar transfers to a native country may be normal remittance behavior and only become suspicious if tied to additional indicators such as structuring or third-party involvement. Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: Recognizing and Reporting Suspicious Activity- Section: Red Flags for Money Services Businesses

NEW QUESTION: 160

Which of the following is a broader risk specific to casinos and gambling?

- A. Low thresholds for transactions
- B. Frequent use of cash
- C. Cross-border transactions
- D. Weak KYC policies and procedures

Answer: ([SHOW ANSWER](#))

Weak KYC policies and procedures represent a broader and more systemic risk specific to casinos and gambling. Without strong KYC, it becomes easier for individuals to engage in money laundering by exploiting anonymity and lack of oversight, regardless of transaction size or method.

NEW QUESTION: 161

Technology has the potential to increase the efficiency and effectiveness of AML/CFT workflows by:

(Select Two.)

- A. Eliminating backlogs through the ability to process large volumes of data
- B. Minimizing privacy concerns through minimized human intervention
- C. Minimizing human intervention in repetitive tasks, increasing data accuracy
- D. Allowing for automatic one-stop searches at the front end by analysts

Answer: ([SHOW ANSWER](#))

Technology plays a critical role in strengthening AML/CFT programs by improving efficiency, consistency, and scalability. Regulators encourage the responsible use of technology while maintaining governance and oversight.

One major benefit is processing large volumes of data efficiently, helping institutions eliminate investigative backlogs and manage increasing transaction volumes. Technology also automates repetitive tasks, reducing human error and improving data accuracy, allowing compliance professionals to focus on higher-value investigative work.

Technology does not eliminate privacy concerns, and front-end search tools alone are not sufficient to drive effectiveness. Human oversight remains essential for decision-making, investigations, and regulatory reporting.

NEW QUESTION: 162

The transaction monitoring system of a bank generated an alert for a car wash client. After making large cash deposits, the client orders international wire transfers.

Which additional circumstances would make the case more suspicious?

- A. The beneficiary of the wire transfers is a foreign company whose shareholders and director are other companies
- B. The wire transfers are for different amounts but with the same beneficiary
- C. The beneficiary of the wire transfer is a resident of a grey-list country
- D. The beneficiary of the wire transfers is a resident of a foreign country bearing the same family name as the business owner

Answer: ([SHOW ANSWER](#))

The suspicion increases when the beneficiary is a foreign company whose shareholders and director are other companies, as this can indicate the use of layered corporate structures to obscure the ultimate beneficial owner and conceal illicit fund flows.

NEW QUESTION: 163

A large international bank is conducting a comprehensive review of its risk management framework to ensure it effectively addresses various financial crime risks, including AML, CFT, sanctions, fraud, anti-bribery and corruption (ABC), and tax evasion.

The bank's compliance team is responsible for evaluating the current risk assessment processes, identifying potential gaps, and recommending enhancements to better mitigate these risks. During

this review, the team needs to consider the different types of risk assessments and how to integrate findings into the overall risk management strategy.

Which approach should the compliance team prioritize to enhance the bank's ability to identify, assess, and mitigate the identified risks?

- A.** Use a static risk assessment model that remains unchanged until a significant regulatory update occurs to ensure consistency in the evaluation process over time
- B.** Delegate the risk assessment process to individual business units to conduct independently and allow for specialized assessments tailored to each unit's specific activities
- C.** Conduct a periodic enterprise-wide risk assessment that includes identifying inherent risks, evaluating the effectiveness of existing controls, and determining residual risks
- D.** Focus primarily on AML risk assessments, as these are typically the most scrutinized by regulators, while addressing other financial crime risks only when issues are identified

Answer: ([SHOW ANSWER](#))

Conducting a periodic enterprise-wide risk assessment (EWRA) is the most effective approach to identifying, assessing, and mitigating financial crime risks. It ensures all inherent risks across areas like AML, CFT, sanctions, fraud, ABC, and tax evasion are evaluated, existing controls are assessed, and residual risks are identified. This comprehensive view enables a cohesive and proactive risk management strategy aligned with regulatory expectations.

NEW QUESTION: 164

Interactions between the compliance department and other functions or departments within an organization contribute to making the anti-financial crime (AFC) compliance program more robust by addressing specific risk areas.

Which departments play a crucial role in enhancing the AFC compliance program of an organization? (Select Two.)

- A.** Information security office (ISO)
- B.** Marketing and sales
- C.** Human resources (HR)
- D.** Data privacy office (DPO)

Answer: ([SHOW ANSWER](#))

* A (ISO): Ensures information security controls are aligned with AFC efforts, protecting sensitive data and reducing the risk of cyber-enabled financial crime.

* D (DPO): Helps ensure compliance with data privacy laws and enables secure, lawful information- sharing for AML purposes.

* "Collaboration with the ISO and DPO is critical to maintaining data security and privacy within AFC compliance frameworks."(CAMS 6th Edition, Governance and Cross-Functional Collaboration) References:

CAMS 6th Edition, Governance and Controls

FATF Guidance on Data Protection and Information Sharing

NEW QUESTION: 165

Which red flag is most relevant to money laundering through capital markets?

- A. A trading customer maintains a portfolio of securities concentrated in one specific emerging market
- B. A security sees a transactional pattern of a steady decrease in both trading volume and prices
- C. A low-priced security sees a sudden spike in investor demand with a rising price
- D. A firm sees an unexpected increase in demand for electronically traded funds

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 166

A financial institution is exploring automation to assist investigators in reviewing flagged transactions.

Currently, investigators spend a significant amount of time gathering data from multiple sources. Which of the following automation features would be most effective in improving investigator efficiency?

- A. Pre-populated templates for SAR filing
- B. Integration of open-source tools to gather real-time intelligence
- C. Automated case prioritization based on risk scoring
- D. AI-powered dashboards summarizing flagged transactions

Answer: ([SHOW ANSWER](#))

AI-powered dashboards summarizing flagged transactions are the most effective feature for improving investigator efficiency, as they consolidate and present relevant data from multiple sources in a structured, actionable format - reducing time spent on manual data gathering and enabling quicker decision-making.

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**)

Special Discount Code: [freecram](#))

NEW QUESTION: 167

Which of the following serves as an example of a successful public-private partnership (PPP)?

- A. The Financial Action Task Force (FATF)
- B. The AUSTRAC Fintel Alliance
- C. The Egmont Group
- D. The Wolfsberg Group

Answer: ([SHOW ANSWER](#))

The AUSTRAC Fintel Alliance is a successful example of a public-private partnership (PPP). It brings together government agencies and private sector organizations to collaborate on detecting, preventing, and disrupting financial crime through shared intelligence, technology, and expertise.

NEW QUESTION: 168

A periodic review has been completed for an existing virtual asset service provider (VASP) customer.

Which of the following are indicators of potential money laundering? (Select Three.)

- A.** Use of shell companies for deposits and withdrawals into the VASP
- B.** Using a peer-to-peer network to reduce costs associated with server maintenance and data storage
- C.** Rapid market fluctuations resulting in quick changes in the value of underlying assets
- D.** Frequent use of mixers and tumblers for holdings and transactions
- E.** Receiving funds from countries known for weak money laundering regulations and frameworks

Answer: ([SHOW ANSWER](#))

Virtual Asset Service Providers (VASPs) are considered higher-risk customers due to their exposure to anonymity, speed, and cross-border transactions. FATF guidance highlights several red flags indicative of potential money laundering activity.

The use of shell companies to move funds into and out of a VASP is a strong indicator of attempts to conceal beneficial ownership and obscure transaction flows. Similarly, frequent use of mixers and tumblers is a well-recognized technique used to break transaction trails and hinder blockchain tracing.

Receiving funds from jurisdictions with weak AML frameworks significantly increases geographic risk, particularly when combined with other red flags.

By contrast, peer-to-peer infrastructure use and market volatility are inherent features of the virtual asset ecosystem and do not, on their own, indicate money laundering.

NEW QUESTION: 169

Which method could be used in the placement stage of money laundering in the real estate sector?

- A.** Paying an invoice to a media company via online banking for property marketing
- B.** Using a registered trust to transfer ownership
- C.** Using cash to purchase property
- D.** Bringing a property back to market quickly after purchasing it

Answer: **C** ([LEAVE A REPLY](#))

Money laundering typically occurs in three stages: placement, layering, and integration. The placement stage involves introducing illicit funds into the financial system.

In the real estate sector, using cash to purchase property is a classic placement method. Cash payments allow criminals to inject large amounts of illicit proceeds directly into high-value assets, often bypassing traditional banking scrutiny.

Using trusts to transfer ownership and rapidly reselling property are more commonly associated with layering or integration, where ownership and transaction complexity is used to disguise the origin of funds. Paying routine invoices via online banking is consistent with legitimate business activity and does not represent placement.

Therefore, cash purchases of property most directly align with the placement stage of money laundering.

NEW QUESTION: 170

A financial institution's US Branch receives a subpoena from law enforcement requesting detailed records of a customer's account activity. The customer is part of an ongoing investigation into a money laundering operation. At the same time, the institution has received a FinCEN 314(b) information-sharing request from another bank seeking details on transactions linked to the same customer. The compliance team is tasked with responding to both the subpoena and the FinCEN 314(b) request. What should the compliance officer prioritize in responding to these requests while ensuring that all legal and regulatory obligations are met?

- A. Notify the customer of the information-sharing request from the other financial institution and seek their consent before responding
- B. Consult the institution's legal counsel to validate the subpoena, then respond directly to law enforcement while ensuring all documentation is properly recorded
- C. Respond to the FinCEN 314(b) request first, as it allows for voluntary information sharing with partner organizations
- D. Provide the requested records to both law enforcement and the other financial institution immediately to ensure full cooperation and transparency

Answer: (SHOW ANSWER)

B: When a subpoena is received, the institution should first consult with legal counsel to ensure the validity and scope of the subpoena. Compliance with law enforcement requests is mandatory and subject to strict legal obligations. All documentation and responses should be properly recorded.

"A subpoena requires a legal response; consult legal counsel to validate the request and respond as required by law." FinCEN 314(b) information-sharing requests are voluntary and can proceed only after fulfilling required legal steps, such as verifying membership in the program and ensuring information-sharing agreements are in place.

CAMS 6th Edition clarifies that "under no circumstances should a customer be notified of a law enforcement inquiry or subpoena." References:

CAMS 6th Edition, Law Enforcement Inquiries and Subpoenas

FFIEC BSA/AML Manual, Information Sharing (Sections 314(a) & 314(b))

NEW QUESTION: 171

Which of the following conditions contribute to a politically exposed person (PEP) posing greater risk than a typical high-risk bank customer? (Select Two.)

- A. The family members and close associates of PEPs may be involved in illicit activities.

- B.** PEPs are granted unlimited credit and financial immunity under international banking regulations.
- C.** PEPs may exploit embassy activities to conceal bribery and corruption transactions.
- D.** PEPs can have illegitimate fund sources but are legally protected from having their accounts closed for activities outside a bank's risk appetite.

Answer: ([SHOW ANSWER](#))

PEPs are recognized by CAMS 6th Edition and FATF as posing elevated risk due to:

- A). The family members and close associates of PEPs may be involved in illicit activities:"The risks extend beyond the PEP to family members and close associates, who may be used to conceal the movement of illicit funds."(CAMS 6th Edition, PEP Risk Factors; FATF Guidance) C).
- PEPs may exploit embassy activities to conceal bribery and corruption transactions:"PEPs may use their position or diplomatic privileges, such as embassy operations, to disguise or facilitate the movement of illicit funds."(CAMS 6th Edition, Corruption and PEP Risks) Incorrect Options:
- B: There is no such legal provision granting PEPs financial immunity or unlimited credit.
 - D: Banks may (and often must) exit PEP relationships not in line with their risk appetite.

References:

CAMS 6th Edition, PEPs and Enhanced Due Diligence

FATF Guidance: PEPs (2013)

NEW QUESTION: 172

Which of the following is a benefit of public-private partnerships (PPP)?

- A.** Sourcing of key resources
- B.** Rapid exchange of information on risks and high-risk activities or persons
- C.** Ensuring understanding of politically exposed persons (PEPs)
- D.** Obtaining salaries in the financial industry

Answer: ([SHOW ANSWER](#))

Public-private partnerships (PPPs) are a key component of modern AML/CFT frameworks and are strongly encouraged by FATF and national regulators. Their primary benefit lies in enhancing timely and effective information sharing between financial institutions, regulators, law enforcement, and financial intelligence units (FIUs).

Through PPPs, authorities can share typologies, red flags, and emerging threat intelligence, while private institutions contribute operational insights derived from real transaction data. This rapid exchange of information on risks, high-risk activities, and suspicious actors significantly improves the detection and prevention of money laundering and terrorist financing.

PPPs do not exist to source staffing resources, provide salaries, or ensure basic understanding of regulatory concepts such as PEPs, which are already addressed through standard AML requirements. Their true value is the speed, quality, and relevance of shared intelligence, allowing participants to respond more effectively to evolving financial crime threats.

NEW QUESTION: 173

When services are provided by a trust and company service provider (TCSP) connected to a high-risk country, which of the following may present an immediate financial crime risk concern?

- A. Management structure
- B. Governance framework
- C. Asset structure
- D. Origin of the funds

Answer: D ([LEAVE A REPLY](#))

The origin of the funds is a primary financial crime risk when dealing with a TCSP connected to a high-risk country. Funds originating from such jurisdictions may be linked to illicit activity, especially if source verification is weak or absent.

NEW QUESTION: 174

Which obliged entities or gatekeepers may be required to perform customer due diligence (CDD)? (Select Four.)

- A. Casino security guards
- B. City court judges
- C. Notaries involved in real estate transactions
- D. Dealers in precious metals and stones
- E. Real estate agents
- F. Accountants and auditors

Answer: ([SHOW ANSWER](#)**)**

FATF standards identify several designated non-financial businesses and professions (DNFBPs) as obliged entities due to their exposure to money laundering risks. These gatekeepers are required to perform customer due diligence (CDD).

Notaries involved in real estate transactions play a critical role in property transfers and are required to identify parties and beneficial owners. Dealers in precious metals and stones handle high-value, portable assets attractive to criminals. Real estate agents facilitate property purchases often used to launder large sums of money. Accountants and auditors may assist in financial structuring, tax planning, or company formation and must conduct CDD when providing covered services.

Casino security guards and judges are not obliged entities under AML/CFT frameworks.

NEW QUESTION: 175

Fuzzy logic or fuzzy matching in the context of name screening is a method that:

- A. Uses machine learning to predict names based on historical data
- B. Matches names on screening lists to names with similar spellings, patterns, or sounds
- C. Matches names with the same length and characters
- D. Relies exclusively on exact string matches

Answer: B ([LEAVE A REPLY](#))

Fuzzy matching is a critical technique used in name screening systems to identify potential matches where names are not spelled identically. Regulators recognize that sanctions, PEP, and

watchlist screening must account for variations in spelling, transliteration, abbreviations, and phonetic differences.

Fuzzy matching algorithms compare names based on similar spelling patterns, phonetics, or character arrangements, allowing institutions to detect matches that exact matching would miss.

This is especially important for names originating from different languages or alphabets.

Exact matching alone is insufficient for effective sanctions screening, as it would fail to capture common variations. While machine learning may enhance screening systems, fuzzy matching itself does not rely on predictive modeling.

Therefore, fuzzy matching improves detection effectiveness while supporting regulatory expectations for robust screening controls.

NEW QUESTION: 176

A compliance officer at a U.S. financial institution receives a grand jury subpoena requesting customer records related to an ongoing money laundering investigation involving a politically exposed person (PEP).

What should the compliance officer do first?

- A.** Notify the customer and seek consent
- B.** Consult with the institution's legal counsel to assess validity and determine the appropriate response
- C.** Immediately provide records to the grand jury
- D.** File a Suspicious Activity Report (SAR) describing receipt of the subpoena

Answer: ([SHOW ANSWER](#))

When a financial institution receives a grand jury subpoena, it is legally compelled to respond, but must do so in a controlled, lawful, and coordinated manner.

The first step is to consult with legal counsel to verify the subpoena's validity, scope, deadlines, and confidentiality requirements. Legal counsel ensures the institution responds accurately, protects privileged information, and complies with applicable laws.

Notifying the customer would constitute tipping off, which is prohibited. Immediate disclosure without legal review may result in over-disclosure or violation of customer privacy laws. Filing a SAR may be appropriate depending on the facts, but it is not the first step and must not reference the subpoena.

This approach aligns with U.S. AML, BSA, and law enforcement cooperation requirements.

NEW QUESTION: 177

What are the rules imposed by the Office of Foreign Assets Control (OFAC) for legal entities and persons related to the US? (Select Two.)

- A.** Any foreign corporation is also penalized if it conducts transactions with sanctioned countries under OFAC rules.
- B.** A foreign individual visiting the US for a short vacation is obligated to follow OFAC rules.
- C.** Nationals of the US must comply with OFAC rules, regardless of where they are located in the world.

D. A subsidiary of a legal entity of the US, which is formally registered in a foreign country, is exempt from OFAC rules.

E. The head office of a foreign legal entity which has a branch in the US does not need to comply with OFAC rules.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 178

Which key performance indicators (KPIs) should be considered in the context of ML/TF transaction monitoring? (Select Three.)

A. Number of days required to hire new staff

B. Number of alerts raised for review or reporting

C. Number of alerts by region

D. Number of transactions by top customers

E. Average time to review an alert

Answer: ([SHOW ANSWER](#))

Key performance indicators (KPIs) are essential for evaluating the effectiveness and efficiency of transaction monitoring systems within an AML/CFT program. Regulators expect institutions to monitor how well their systems identify, prioritize, and resolve suspicious activity.

The number of alerts raised provides insight into system sensitivity and potential over- or under-alerting.

Tracking alerts by region helps institutions identify geographic risk concentrations and emerging threats. The average time to review an alert measures operational efficiency and whether investigations are conducted promptly, as required by regulatory expectations.

Hiring timelines and transaction volumes by top customers are operational or business metrics and do not directly assess transaction monitoring effectiveness.

NEW QUESTION: 179

A bank is using a network analysis tool to identify links between its customers and criminal entities.

The system identifies potential indirect relationships but is unable to prioritize them. What should the compliance officer do to enhance the tool's effectiveness?

A. Manually review all flagged relationships for accuracy

B. Implement risk-scoring algorithms for indirect connections

C. Integrate external databases and social media profiles to cross-check flagged entities

D. Focus on direct connections between customers and criminal entities

Answer: ([SHOW ANSWER](#))

Anti-Money Laundering (AML) regulations and guidance from bodies such as the Financial Action Task Force (FATF) emphasize the importance of a risk-based approach when identifying and managing money laundering and terrorist financing risks. Network analysis tools are commonly used by financial institutions to detect direct and indirect relationships between customers and

known criminal entities. However, without prioritization, these tools may generate large volumes of alerts that reduce operational effectiveness.

Implementing risk-scoring algorithms for indirect connections allows the institution to rank identified relationships based on factors such as proximity to criminal entities, transaction volume, frequency, customer risk rating, and typology relevance. This enhances the tool's effectiveness by enabling compliance teams to focus on the highest-risk relationships first, in line with regulatory expectations for efficient and proportionate controls.

Manually reviewing all flagged relationships is impractical and inconsistent with scalable AML programs.

Integrating external databases or social media profiles may raise data quality, privacy, and governance concerns and is not a primary solution for prioritization. Focusing only on direct connections would weaken the AML framework, as criminals frequently use layered and indirect relationships to conceal illicit activity.

Therefore, applying risk-based scoring methodologies is the most effective and regulator-aligned way to enhance network analysis tools.

NEW QUESTION: 180

Which customer actions are red flags for virtual currency peer-to-peer transactions? (Choose two.)

- A.** A customer receives funds from a popular decentralized mixer
- B.** A customer uses funds from their monthly income to purchase virtual currency
- C.** A customer makes a transaction on the blockchain that their traditional financial institution is unaware of
- D.** A customer receives multiple wires from different sources and uses those funds to purchase virtual currency

Answer: ([SHOW ANSWER](#))

Receiving funds from a decentralized mixer and using multiple incoming wires from different sources to purchase virtual currency are red flags, as they can indicate attempts to obscure the origin of funds and facilitate money laundering through virtual asset transactions.

NEW QUESTION: 181

Which statement regarding data privacy is the most accurate in the context of AML investigations?

- A.** FIUs should document purposes for which personal data included on suspicious activity reports may be shared with other agencies
- B.** Organizations are required to demonstrate that customers have opted into information sharing before submitting suspicious activity reports to relevant financial intelligence units (FIUs)
- C.** Data privacy laws prohibit information sharing between financial institutions for the purposes of AML investigations in all jurisdictions
- D.** Any customer that is the subject of a suspicious report filing has the right to request redaction of their personal data

Answer: **A** ([LEAVE A REPLY](#))

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (447 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 182

Which technologies are commonly used to help financial institutions (FIs) navigate privacy and data protection regulations while securely sharing client information with private third-party entities? (Choose two.)

- A. Blockchain to ensure traceability and security in shared data transactions
- B. Data encryption to protect sensitive information from unauthorized access
- C. Privacy-enhancing technologies (PETs) to enable secure and privacy-compliant data sharing
- D. Artificial intelligence (AI) to automating compliance processes like data anonymization and secure sharing
- E. Cloud storage solutions for efficient data handling and management

Answer: (SHOW ANSWER)

Data encryption protects sensitive information from unauthorized access, while privacy-enhancing technologies (PETs) enable secure and compliant data sharing with third parties, helping financial institutions meet privacy and data protection regulations.

NEW QUESTION: 183

Who bears the ultimate responsibility for approving a financial institution's relationship with a politically exposed person?

- A. Enhanced due diligence compliance officer
- B. Senior management
- C. KYC analyst
- D. Relationship manager

Answer: (SHOW ANSWER)

NEW QUESTION: 184

The United Nations Security Council (UNSC) is empowered to impose sanctions regimes against countries and terrorist organizations.

Which statements are true regarding sanctions imposed by the UNSC? (Select Two.)

- A. Attempts to circumvent or evade sanctions imposed by the UNSC can constitute a criminal offense if designated under local laws and regulations

B. The UN can impose arms embargoes but cannot prohibit direct or indirect exports of other goods to specific countries

C. Member countries of the United Nations are expected to implement and enforce sanctions imposed by the UNSC

D. Direct breaches of sanctions imposed by the UNSC constitute a criminal offense in all member countries

Answer: (SHOW ANSWER)

The United Nations Security Council (UNSC) is authorized under the UN Charter to impose binding sanctions measures on member states. These sanctions may target countries, entities, or individuals and can include arms embargoes, travel bans, asset freezes, and restrictions on trade or financial services.

Statement A is correct:

Circumventing or evading UNSC sanctions may constitute a criminal offense if the jurisdiction has incorporated UN obligations into domestic law. While the UNSC does not directly impose criminal penalties, member states must implement these measures locally, and many jurisdictions have laws that make such violations criminal acts.

Statement B is incorrect:

The UNSC is empowered to impose broad restrictions, including trade bans beyond arms, such as on luxury goods, fuel, or specific commodities. Therefore, the idea that it cannot prohibit exports beyond arms is inaccurate.

Statement C is correct:

Member countries of the United Nations are expected to implement and enforce UNSC sanctions, in accordance with their obligations under the UN Charter (specifically Chapter VII). Countries are responsible for transposing these sanctions into their national legal frameworks.

Statement D is incorrect:

Although member countries are required to enforce sanctions, not all countries automatically consider breaches a criminal offense. Whether a violation is criminal depends on how each country enacts UN sanctions domestically.

Reference: ACAMS CAMS Study Guide - 6th Edition, Chapter: International AML Standards-Section:

United Nations Initiatives and Global Sanctions Framework

NEW QUESTION: 185

Which of the following statements describe the strengths associated with public-private partnerships (PPPs)?

(Choose two.)

A. Public organizations can better understand what the private sector experiences and inform policy and the enactment of laws

B. Data-protection privacy policies provide an opportunity to develop information sharing protocols to prevent unauthorized access to information

C. Data-protection privacy policies prohibit the evolution of PPPs due to restrictions based on legacy government legislation

D. Small business owners can choose third-party providers or financial institutions to keep their private data safe which can easily be shared within a PPP

Answer: ([SHOW ANSWER](#))

Public-private partnerships allow public organizations to gain insights from the private sector to shape effective policies and legislation. Additionally, strong data protection and privacy frameworks help create secure information-sharing protocols within PPPs, enhancing collaboration while preventing unauthorized access.

NEW QUESTION: 186

A financial institution's transaction monitoring system flags an unusually high volume of international wire transfers originating from a small business account. The transfers are being sent to multiple jurisdictions known for limited regulatory oversight. Additionally, an employee reports suspicious behavior from the account holder during an in-person visit, where they requested a large cash withdrawal without providing a clear business justification. As part of the investigation, the compliance team must assess whether this activity is suspicious and determine the appropriate next steps.

Which of the following steps should be taken first in the investigation process to properly gather information and assess whether the transactions are suspicious?

A. Review the transaction history of the account to identify patterns, including the frequency, destination, and purpose of the wire transfers

B. Notify senior management and suggest account closure due to potential risks

C. Immediately file a suspicious activity report (SAR) based on the employee's report of suspicious behavior

D. Contact the customer directly to ask for clarification on the reason for the large cash withdrawal

Answer: ([SHOW ANSWER](#))

A: The first step in any suspicious activity investigation is to review the transaction history and other relevant account information to establish context, identify patterns, and determine if the behavior is consistent with known typologies of money laundering.

"The initial phase of an AML investigation is to review relevant account information and transaction activity to assess whether a SAR filing is warranted." This approach ensures that any subsequent decisions, such as escalation, SAR filing, or customer outreach, are based on a comprehensive understanding of the facts.

References:

CAMS 6th Edition, Suspicious Activity Monitoring and Investigation

FFIEC BSA/AML Manual, Suspicious Activity Reporting

NEW QUESTION: 187

A deficiency in the design of a bank's AML/CFT compliance program could result in placing individual accountability on which part of the regulated entity? (Select Two.)

- A. The compliance department
- B. Board of directors
- C. Product oversight committee
- D. Senior management

Answer: ([SHOW ANSWER](#))

Regulatory frameworks and enforcement actions consistently emphasize individual accountability at the highest levels of governance when AML/CFT compliance programs are deficient in design or implementation.

The board of directors is ultimately responsible for oversight of the institution's AML/CFT framework. This includes approving policies, setting risk appetite, and ensuring that adequate resources and governance structures are in place. Failure to fulfill these responsibilities can result in regulatory findings and personal accountability.

Senior management is responsible for implementing the board-approved AML/CFT strategy and ensuring that controls operate effectively in practice. This includes overseeing compliance functions, addressing identified weaknesses, and ensuring timely remediation. Deficiencies in program design-such as inadequate risk assessments or ineffective controls-often lead regulators to hold senior management accountable.

While the compliance department plays an important role in execution and advisory functions, accountability for program design and effectiveness rests with the board and senior management, not committees or individual departments.

NEW QUESTION: 188

Benefits of using artificial intelligence (AI) in conjunction with or in place of traditional rules-based transaction monitoring include that AI can: (Select Two.)

- A. Increase the number of false positive alerts
- B. Create unbiased scenarios during the machine training phase
- C. Identify changes in customer behavior to more accurately assess risk
- D. Generate customer risk scores to predict potential financial crime activity

Answer: ([SHOW ANSWER](#))

Artificial intelligence (AI) enhances transaction monitoring by complementing or improving upon traditional rules-based systems. Regulators recognize that AI can strengthen AML programs when deployed with appropriate governance and oversight.

One key benefit is the ability to identify changes in customer behavior over time. AI models analyze historical and real-time data to detect deviations from expected patterns, allowing institutions to reassess customer risk more dynamically and accurately.

AI can also generate predictive customer risk scores, helping institutions prioritize alerts and focus investigative resources on higher-risk customers and activities. This improves efficiency and effectiveness while supporting a risk-based approach.

AI is designed to reduce false positives, not increase them, and bias must be carefully managed during training through governance and data controls.

NEW QUESTION: 189

An international bank is investigating a payment requested by one of its correspondent relationships that generated an alert in the automated transaction monitoring system. The payment originated from a corporation located in Hong Kong and the final beneficiary is an individual located in New York.

Which steps should the bank take first to address the alert? (Select Three.)

- A. Send a 314(b) request to the corporation's bank in Hong Kong
- B. Call the receiving individual to review identity verification documents
- C. Check for negative news in public sources on the sender and receiver
- D. Confirm that neither the beneficiary nor the originator are sanctioned parties
- E. Request supporting documents, including invoices and contracts to confirm the purpose of the payment

Answer: C,D,E ([LEAVE A REPLY](#))

NEW QUESTION: 190

A large international bank's chief compliance officer (CCO) is exploring ways to enhance the bank's ability to identify suspicious activities by using intelligence data more effectively. One potential solution is to engage in public-private partnerships (PPPs) to leverage shared intelligence and enhance collaboration with government agencies.

The bank considers joining a PPP initiative with the local Financial Intelligence Unit (FIU) and other financial institutions to improve its access to relevant data and intelligence. The CCO understands that while PPPs can provide significant benefits, such as improved risk detection and enhanced information sharing, there are also potential limitations, including data privacy concerns and differing priorities between public and private sector partners.

Which approach would best maximize the benefits of PPPs for the bank while mitigating the limitations associated with data sharing and intelligence?

- A. Engage in the PPP without strict data sharing protocols, allowing for open and unrestricted flow of information between the bank, FIUs, and other financial institutions
- B. Rely solely on the intelligence provided by government agencies through the PPP because they have the most comprehensive data on suspicious activities
- C. Establish a clear framework within the PPP that outlines data privacy protections and ensures that information sharing complies with legal and regulatory requirements in all jurisdictions involved
- D. Prioritize the bank's internal data sources over external intelligence from PPPs, as internal data is easier to control and does not present data privacy challenges

Answer: ([SHOW ANSWER](#))

To maximize the benefits of PPPs while addressing data privacy and regulatory concerns, the bank should establish a clear framework within the partnership that defines privacy protections and ensures all information sharing complies with applicable legal and regulatory requirements

across jurisdictions. This approach fosters trust, enables effective collaboration, and mitigates potential legal risks.

NEW QUESTION: 191

The effectiveness of AML/CFT measures can be best measured by the extent to which systems and controls:

- A. Comply with relevant laws and regulations
- B. Minimize operational burden placed on the financial institution
- C. Mitigate the risks and threats of financial crime
- D. Are implemented in a cost-effective way

Answer: ([SHOW ANSWER](#))

While regulatory compliance, cost efficiency, and operational considerations are important, the primary objective of AML/CFT measures is to reduce and manage the risks and threats of financial crime.

FATF emphasizes that effectiveness should be measured by outcomes, not merely by technical compliance.

An AML/CFT framework may fully comply with laws and still be ineffective if it fails to detect, deter, or disrupt money laundering and terrorist financing. Regulators increasingly focus on whether systems and controls actually identify suspicious activity, prevent misuse of the financial system, and support law enforcement efforts.

Minimizing operational burden and controlling costs are secondary considerations and must not compromise risk mitigation. A cost-effective system that fails to detect financial crime would not meet regulatory expectations.

Therefore, the true measure of effectiveness lies in how well systems and controls mitigate financial crime risks and threats in practice.

NEW QUESTION: 192

Which should be provided to the board of directors or designated specialized committee when preparing suspicious activity reports (SARs)?

- A. Copies of all SARs filed during the reported period
- B. All possible details of SARs filed during the reported period
- C. Statistical data regarding SARs filed during the reported period
- D. Names of all customers subject to SARs filed during the reported period

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 193

An employee in a corporation's finance department hears news of an internal investigation into potential fraud within the company, quits her job, and disappears.

If they had been observed before her resignation, which characteristics of the employee would have been considered red flags? (Select Two.)

- A. The employee was originally from a high-risk jurisdiction

- B. The employee had friends in high-risk industries
- C. The employee had a lavish lifestyle for her income
- D. The employee was constantly evasive about the reasons for leaving her previous corporate finance job

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 194

A risk-based approach (RBA) means that countries, competent authorities, and financial institutions:

- A. Are exempt from mitigating AML/CFT risks assessed as low
- B. Are expected to reduce all residual risks to low
- C. Are expected to identify, assess, and understand the AML/CFT risks to which they are exposed
- D. Will allocate compliance resources to non-compliance-related tasks

Answer: ([SHOW ANSWER](#))

The risk-based approach (RBA) is a foundational principle of FATF standards. It requires countries, regulators, and financial institutions to identify, assess, and understand their money laundering and terrorist financing risks.

Once risks are understood, entities must apply proportionate mitigation measures. Higher risks require stronger controls, while lower risks may justify simplified measures. However, no risk is ignored or exempted from mitigation.

Regulators do not expect all residual risks to be reduced to low; rather, risks must be managed within an acceptable risk appetite. Resource allocation under an RBA prioritizes AML/CFT activities, not unrelated tasks.

Therefore, the correct definition of an RBA focuses on understanding and managing risk proportionately.

NEW QUESTION: 195

A basic principle of the Egmont Group is to:

- A. Publish standards for reporting suspicions
- B. Facilitate the organization of regulatory authorities
- C. Publish decisions taken on international investigations
- D. Arrange information-sharing protocols between Financial Intelligence Units (FIUs)

Answer: ([SHOW ANSWER](#))

The Egmont Group is an international network of Financial Intelligence Units (FIUs) established to promote cooperation and information exchange in the fight against money laundering and terrorist financing. One of its core principles is to facilitate secure, timely, and lawful information sharing between FIUs.

The Egmont Group provides a framework, standards, and secure channels-such as the Egmont Secure Web-that allow FIUs to exchange intelligence related to suspicious transactions,

typologies, and emerging financial crime risks across borders. This cooperation is essential given the transnational nature of money laundering and terrorist financing.

The Egmont Group does not publish reporting standards, act as a regulator, or publicly disclose investigation outcomes. Its role is operational and intelligence-focused, supporting FIUs while respecting confidentiality and national legal frameworks.

Therefore, arranging information-sharing protocols between FIUs is a fundamental principle of the Egmont Group.

Valid CAMS7 Dumps shared by EduDump.com for Helping Passing CAMS7 Exam!

EduDump.com now offer the **newest CAMS7 exam dumps**, the EduDump.com CAMS7 exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com CAMS7 dumps with Test Engine here:

<https://www.edudump.com/exams/ACAMS/CAMS7/premium/> (**447** Q&As Dumps, **35%OFF**

Special Discount Code: freecram)