ACAMS.CAMS-KR.v2025-03-03.q354

□□□□:	CAMS-KR
□□□□:	Certified Anti-Money Laundering Specialists (CAMS Korean Version)
□□□:	ACAMS
□□ □□ □□□:	354
□□:	v2025-03-03
# □□ □:	2085
# □□ □□□:	3540
https://www.krdump.com/ACAMS.CAMS-KR.v2025-03-03.q354.html	

NEW QUESTION: 1
□□ □□□ □□ EU □□□ □□ □□□ □□□□□□?
A. □□□□□ □□□ □□ EU □□□ □□□ □□ □□ □□
B. □□ □□□ □□□ □□ EU □□□□□ □□ □□□ □□□□□□.
C. □□□□□ EU □□□□□□□□(FIU)□ □□□□□ □□ □□□ □□□ □ □□□ □□
D. EU □□□□□ □□□□□ □□□ □□ □□□□□ □□□□□(FI) □□□□□ □□
Answer: (SHOW ANSWER)
The key goal of EU Directives on money laundering is to establish a consistent regulatory environment across the EU to prevent money laundering and terrorist financing, and to align EU policy with international standards and best practices. EU Directives are legal acts that set out the objectives and principles that member states must achieve, but leave the choice of methods and measures to the national authorities. EU Directives on money laundering aim to harmonize the rules and obligations for FIs and other obliged entities in the areas of customer due diligence, record-keeping, reporting, supervision, and sanctions. They also aim to address the emerging threats and vulnerabilities of the financial system, such as the use of virtual assets, prepaid cards, high-risk third countries, and beneficial ownership. By creating a consistent regulatory environment across the EU, the Directives seek to enhance the effectiveness and cooperation of the AML/CFT regime, and to protect the integrity and stability of the internal market and the financial system.
Reference:
1: Guide to EU Anti Money Laundering Directives (AMLD) - ComplyAdvantage1
2: Directive - 2015/849 - EN - Fourth Anti-Money Laundering Directive - EUR-Lex2
3: EU context of anti-money laundering and countering the financing of terrorism3

NEW QUESTION: 2
□□ □□(EU) □□□ □□ □□□ □□□□□□ □□ □ □□□ □□□□□ □□□□□ □□□ □□ □ □□ □□□□□ □□□□□. □□ □□□ □□□ □□ □□□□□ □□□ □ □□ □□□ □□ □□□□□

□□ □□□ □□□ □3□□ □□□ □ 7,500□ □□□ □□□ □□□ □□ □□□□ □□□ □□ □□□. □□ □□□ □□□ □□□□ □□□□□ □□ □□ □□ □□□□ □□ □□□□ □□□ □□.

□□ □□ □□ □□ □□ □□□ □□□ □ □□ □ □□ □□ □□□ □□□□□? (2□□ □□□ □□.)

A. □3□ □□□□ □□ 7,500□ □□ □□

B. □□□□□ □□□□□ □□□□ □□□□

C. EU □□□□ □□ □□□ □□ □□□ □□ □□□□ □□ □□

D. □□ □□□□□□ □□□□□ □□ □□ □□□ □□ □□□□.

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

According to the ACAMS study guide1, some of the common red flags for money laundering or financing terrorism are:

Customers who provide insufficient or suspicious information, such as unusual or unverifiable identification documents, different taxpayer identification numbers, or vague or inconsistent information about their business or source of funds.

Transactions that have unusual features, such as large cash payments, unexplained payments from a third party, use of multiple or foreign accounts, complex or illogical transactions, or transactions that are inconsistent with the customer's profile or expected behavior.

Geographic concerns, such as transactions involving high-risk jurisdictions, offshore financial centers, secrecy havens, or countries subject to sanctions or embargoes.

Ultimate beneficial ownership that is unclear, such as customers who use shell companies, trusts, or other legal entities to obscure their identity or the identity of the true owners or controllers of the funds or assets.

In this scenario, two red flags that could indicate money laundering or financing terrorism are:

B . The guarantor company's ownership structure is overly complex. This could be an attempt to hide the true source or destination of the funds, or to evade regulatory or law enforcement scrutiny. The use of a trust formed in a Caribbean island and a holding company based in a European secrecy haven could also indicate geographic concerns, as these jurisdictions are known for their low transparency and high confidentiality.

D . The ultimate beneficial owner is a young lady who has gained her wealth through a small business. This could be a case of false or misleading information, as the source of funds is not commensurate with the size or nature of the transaction. The fitness studio business could be a front or a cover for illicit activities, or the young lady could be a nominee or a straw man for the real owner or beneficiary.

NEW QUESTION: 3

□□□□□ □□□□□ □□□ □□ □□ □□□ □□□ □ □□□□ □□□ □ □ □□ □□□ □ □□□□?

A. □□ □□□ □□□□□□□(FIU) □□□□ □□□□ □□□□□ □□□□□ □□□ □□□ □ □□□□□□ □□ □□□ □□□□.

B. □□□□□□ □□□□□□ □□□ □□□ □□ □□, □□□ □□, □□□ □□□□□□ □□□ □□ □□□.
C. □□, □□, □□□ □□□□□□ □□ □□□ □□□ □□ □□ □□□ □□□□□ □□□□□□.
D. □□□ □□□, □□ □□ □□□, □□ □□□□□ □□□ □□ □□□ □□□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The first step in a financial investigation is to review and analyze all internal sources of information related to the suspicious transaction.
Option C (Correct): Gathering and assessing internal data helps investigators establish a baseline for normal vs. suspicious customer behavior. This includes reviewing KYC (Know Your Customer) documentation, transaction history, and any previous alerts on the customer.
Option B (Incorrect): This is part of the investigation, but an investigator first needs to gather data before determining consistency with expected behavior.
Option A (Incorrect): An FIU is typically contacted after internal analysis has been completed and a Suspicious Activity Report (SAR) is warranted.
Option D (Incorrect): External information is useful, but internal data should be reviewed first to confirm whether a case needs escalation.

NEW QUESTION: 4
□□□, □□□, □□, □□ □ □□□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □ □□□□□? 3□□ □□□ □□□□□
A. □□□ □□ □□□ □□□ □□ □□ □□□□ □□□ □□ □□□□ □□□□□ □□□ □□□ □ □□ □□□□□□ □□□□□□.
B. □□ □□ □□ □ □□□ □□□ □□□□□ □□ □□
C. □□□□□□□ □□ □□□ □□ □□□ □□□.
D. □□ □□□□□□ □□□ □□□□ □□ □□□□□ □□□ □□□ □□□□□□ □□□□□□ □□□ □□.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 5
□□□□□ □□ □□ □□□ □□ □□□ □□, □□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□□□ □□□ □□ □□□ □□□□□□□. □□ □□□□□□ □□□□□
□□ □□□□□□ □□□ □□□□□□ 8□□□ □□□□□. □□ □□□□□ □□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□□□ □□□□□□□ □□□□□□. □ □□□ □□ □□ □□ e-□□ □□□ □□□□□□□.
□□ □ □□ □□□□□ □□ □□□ □□ □□□ □□□□□□?
A. □□□□□ □□□ □□ □□□ □□□ □□□ □□□.
B. □□□ □□□□□ □□ □□□ □□□□□□ □□□□□ □□□.
C. □□ □□□ 6□□ □□□ □□□□□□□□ □□□□□ □□ □□□ □□□□□ □□□.
D. □□ □□ □□□□□ □□ □□□□□ □□□□□ □□ e-□□□ □□ □□□□□□.
Answer: (SHOW ANSWER)

The internal review would most likely recommend that the institution provide product-specific anti-money laundering training to all relevant employees, not just actuaries. This is because life insurance products can be used for money laundering purposes, such as purchasing policies with illicit funds, surrendering policies for cash value, or using policies as collateral for loans. Therefore, all employees who are involved in selling, servicing, or processing life insurance products should be aware of the money laundering risks and red flags associated with these products, and how to report any suspicious activity. The institution should also ensure that the training is timely, effective, and tailored to the specific roles and responsibilities of the employees.
The other options are not as relevant or appropriate as the correct answer. Option A is too broad, as not all staff need to be trained on anti-money laundering, only those who are relevant to the institution's business activities and exposure to money laundering risks. Option C is too narrow, as it only focuses on actuaries and does not address the need for training other employees who may deal with life insurance products. Option D is not sufficient, as e-learning alone may not be effective in ensuring that employees understand and retain the anti-money laundering content, and the institution should also conduct follow-up assessments to measure the impact and outcomes of the training.
Reference:
ACAMS Study Guide for the CAMS Certification Examination - 6th Edition, Chapter 3: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), page 57.
ACAMS CAMS Certification Video Training Course, Module 3: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Lesson 3.5: Training and Testing.
Best Practices for Anti-Money Laundering Compliance - DIRO Original, Section 3: Adequate Training.

NEW QUESTION: 6
□□ □□ □□□□ □□ □□□ □□ □□ □ □□ □□□ □□□ □□ □□□□□?
A. □□□□□ □□
B. □□ □□ □□□ □□ □□
C. □□□ □□□□ □□
D. □□□□□ □□ □□ □□
Answer: (SHOW ANSWER)
The correct answer is B. Questioning reporting requirements. When a prospective customer questions reporting requirements during the account opening process, it may raise concerns about their intentions or understanding of anti-money laundering (AML) regulations. Financial institutions should investigate further to ensure compliance and assess any potential risks associated with the customer's behavior1.
Reference:
1. FDIC: Customer Identification Program
2. Financial Crime Academy: USA PATRIOT Act Customer Identification Program

3. BankersOnline: Lending and Customer Identification Programs

NEW QUESTION: 7

□□ □□□□ □ □□ □□(LEA)□ □□ □□(FI)□ □□ □ □ □□ □□□□ □□ □□(FI)□ □ □□□□. LEA□ □□□□ □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□□□□. FI□ □□□ □□ □□□? (2□□ □□□□□.)

A. □□□□□□□ □□□ □□□□ □□□□□ □□□ □□□ □□□□ □□ □□ □□□□□.

B. □□□ □□□ □□ □□□ □□□□ □□□ LEA□ □□□□.

C. □□ □□□□ □□ □□□□ □□ □□□ □□ □□□□□□.

D. □□ LEA □ □□ □□□ □□ □□□ □□□□.

E. □□□ □□□ □□□ □□ □□ □□□ □□ □□□□□□.

Answer: A,D (LEAVE A REPLY)

According to the Certified Anti-Money Laundering Specialist (the 6th edition), the financial institution (FI) should take the following actions:

A . Review the client's activity, determine if suspicious activity exists, and report accordingly. The FI should assess the risk of the situation and determine if there is any suspicious activity that needs to be reported to the appropriate authorities. This would involve conducting a review of the client's account activity and transactions to determine if there are any indicators of money laundering or terrorist financing.

D . Inform local LEA and regulator of the request for awareness. The FI should inform the local law enforcement agency and regulator of the request from the foreign jurisdiction to raise awareness of the situation and determine if any further actions need to be taken.

NEW QUESTION: 8

MSB(Money Services Business)□ □□ □□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □?

A. MSB□ □□ □□□□□□ □□□ □□□ □ □□□□ □□□.

B. MSB□ □□□□□ □□□ □□□□ □□□□□ □□ □□□□ □□□□□ □□□□□ □□□ □□□.

C. MSB□ □□□□ □□□ □□□ □□□ □□ □ □□□□.

D. MSB□ □□□□ □□ □□ □□ □□ □□□□□.

Answer: (SHOW ANSWER)

MSBs are frequently accused of being high risk for money laundering because they offer services that can facilitate the movement and conversion of illicit funds, such as currency exchange, money transmission, cheque cashing, and online payment. However, not all MSBs pose the same level of risk, and the degree of regulatory oversight and compliance requirements for MSBs may differ significantly depending on the jurisdiction they operate in. Some countries may have robust anti-money laundering (AML) regimes for MSBs, while others may have weak or inconsistent regulations, or even no regulations at all. This creates challenges and vulnerabilities for MSBs that operate across borders, as they may face different expectations and obligations from different authorities, or encounter gaps or loopholes in the AML framework. Moreover, some

MSBs may operate informally or illegally, without registering or obtaining licenses from the relevant regulators, making them harder to detect and supervise. Therefore, MSBs are often perceived as high risk for money laundering, as they may be exploited by criminals who seek to take advantage of the regulatory discrepancies or deficiencies among countries.
Reference:
Understanding risks and taking action for money service businesses1
What Is A Money Services Business?2
Money Services Business (MSB) Information Center3
Money Services Business (MSB): Types, Examples, & AML Compliance4

NEW QUESTION: 9
□□□□ □□ □□ □□□□ □□□ □□□ □□ □□ □□ □□□ □□□ □ □□□□.
A. □□□□ □□□□□ □□□□.
B. □□□ □□□ □□□□ □□□□□.
C. □□ □□ □□ □□□□ □□□□ □□□ □□□ □□□□□.
D. □□□ □3□□ □□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
purchasing a low volume of chips with cash and turning them in for a casino check is a common technique of money laundering in casinos. This method allows the launderer to convert "dirty" money into physical casino chips, which are then played with for a short while, and then cashed out as "clean" money in the form of a check. This way, the launderer can avoid the reporting requirements and the traceability of cash transactions.
Reference:
ACAMS CAMS Certification Video Training Course - Exam-Labs1
Understanding Money Laundering in Casinos | ComplyAdvantage2
Casino Money Laundering: Red Flag Indicators - Alessa3

NEW QUESTION: 10
□□ □□ □□ □□□□ □□□□□ □□□ □ □□ □ □□ □□□□□ □□□ □□□□ □□□
□□□□ □□□ □□□□□□.
□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□ □□ □□
B. □□□ □□□□ □□□ □□□□ □□□□ □□□□ □□□□
C. □□□ □□□□ □□□ □□□ □□ □□ □□□□ □□□□ □□□□□
D. □□□ □□□□ □□□ □□□ □□ □□ □□□□ □□□□ □□ □□ □ □□ □□
Answer: (SHOW ANSWER)
A customer's account appears to function as a funnel account whereby cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made

NEW QUESTION: 11

□□□ □□□□□□ □□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□
□□ □□□□□. □□□ □□□□□□□ □□□ □□ □□ □ □□ □□□ □□ □ □□□ □□□□□
□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□
□□□ □□□□ □□□?
1. □□□ □□ □□□□□□□□□ □□□ □□□ □□□□ □□□ □□□□□□.
2. □□ □□□ □□□□□.
3. □□□ □□□ □□ □□□ □□□ □□□□□□.
4. □□□ □□□ □□□□ □□□ □□□ □□□□□□.
A. 1, 2, 3□
B. 1, 2, 4□
C. 1, 3, 4□
D. 2, 3, 4□
Answer: D (LEAVE A REPLY)
The anti-money laundering specialist should recommend a financial institution to investigate the source of funds, identify people and companies that are clearly related, and identify a person fully, including their political history, when dealing with individuals holding important public positions. These are essential steps to conduct enhanced due diligence based on public information, as they can help to assess the risk profile, the legitimacy, and the transparency of the customer relationship. The Basel Committee on Banking Supervision's list of public officials is not a reliable source of public information, as it is not comprehensive, updated, or verified. Therefore, it is not a sufficient criterion to check the background of potential customers.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 4, page 971
ACAMS CAMS Certification Video Training Course, Module 4, Lesson 32
ACAMS CAMS Certification Exam Outline, Domain 4, Task 23

NEW QUESTION: 12
EU□ □6□ □□□□ □□ □□(6AMLD):
A. □□□□□□ □□□□ □□ □□ □□□ □□ AML □□ □□.
B. □□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□.
C. □□□□□ □□□□ □□ EU □□□□□□□ □□□□□□.
D. □□ □□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
The 6th AML Directive (6AMLD) introduced tighter rules to combat financial crime, particularly around beneficial ownership transparency.
Option D (Correct): 6AMLD enhances transparency by requiring accurate and verified data in central beneficial ownership registries, making it harder to hide illicit funds behind shell companies.
Option A (Incorrect): While some entities face increased scrutiny, crowdfunding platforms and football clubs were not the primary focus of 6AMLD.

Option B (Incorrect): 6AMLD does not remove the EU's obligation to conduct risk assessments; risk-based approaches remain central to AML efforts.
Option C (Incorrect): The EU AML Authority (AMLA), planned for 2024, will centralize enforcement, but 6AMLD did not create this entity.

NEW QUESTION: 13
□□ □□ □ □□□□□ □□□□□ □□ □ □□ □□□ □□□□□□?
A. □ □□ □□□ □□ □□ □□ □□
B. □□ □□ □□□ □□□□□□ □□□□.
C. □ □□ □□□ □□□ □□ □□□ □□ □□□
D. □□□ □□□ □□□ □□
Answer: B,C,D (LEAVE A REPLY)
During an internal investigation, employees should be instructed to do the following actions:
Inform counsel of all request for documentation: This is to ensure that the legal rights and obligations of the organization and the employees are protected and respected. Counsel can also advise on the scope, relevance, and confidentiality of the requested documents1.
Make copies of all documents provided to law enforcement: This is to maintain a record of the information that has been disclosed and to prevent any loss or alteration of the original documents. Copies should be made before the documents are handed over to law enforcement2.
Keep a log of the documents requested: This is to track the progress and status of the investigation and to avoid any duplication or omission of the requested documents. The log should include the date, time, description, and location of the documents, as well as the name and contact details of the person who requested and received them3.
Providing corporate documents directly to law enforcement, on the other hand, is not an action that employees should be instructed to do during an internal investigation. This is because law enforcement may not have the legal authority or the proper warrant to access the documents, and doing so may violate the privacy or confidentiality of the organization or the employees.
Employees should consult with counsel before providing any documents to law enforcement4.
Reference:
1: Internal money laundering reporting | The Law Society5 2: How to Conduct Effective AML Investigations - Blog | Unit212 3: What Is The Importance Of An Internal Investigation?4 4: Anti-Money Laundering: 5 Steps to Conduct an Audit3

NEW QUESTION: 14
□□ □□ □□□□ □□ □□□□□□□ AML □□ □□□ □□ □□ □□□ □□□□ □□□□ □ □□ □□□□□□□. □□ □□ □□□□ □□□ □□ □□□ □□□ □□□?
A. AML □□ □□□ □□□ □□□□□□ □□□□□.
B. □□ □□ □□ □□□ □□□□.
C. □□ □□□□ □□ □□□ □□□□.
D. □□ □□□ □□ □□ □□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)

The Head of Compliance is responsible for overseeing and managing the AML compliance program of the organization. When an external auditor identifies a finding that indicates a failure to comply with a regulatory requirement, the Head of Compliance should take prompt and appropriate action to address the issue and prevent recurrence. The best course of action is to submit a corrective action plan with a target timeline to the auditor and the relevant regulator, demonstrating the organization's commitment to remediate the finding and improve its AML compliance program. The corrective action plan should include the root cause analysis of the finding, the specific actions to be taken, the responsible parties, the expected outcomes, and the deadlines for completion. The Head of Compliance should also monitor the progress of the corrective action plan and report any updates or challenges to the auditor and the regulator.
Reference:
JPMorgan Chase & Co. Global Anti-Money Laundering Compliance Program, page 2: "The Firm's Global Head of Financial Crimes Compliance is responsible for overseeing the implementation and effectiveness of the AML Program and reports to the Firm's Chief Compliance Officer. ... The Global Head of Financial Crimes Compliance is also responsible for ensuring that the Firm responds appropriately to any regulatory inquiries, examinations, or investigations relating to AML matters, and that any identified issues or deficiencies are promptly remediated." The Board's Role in AML Compliance, Section "Board Oversight of AML Compliance Program": "The board should also ensure that the institution has a process in place to identify, report and correct any compliance deficiencies or violations in a timely manner. This includes ensuring that the institution responds to any regulatory inquiries, examinations or enforcement actions, and implements any required corrective actions." AML Compliance Officer: the Role, Skills, and Responsibilities, Section "AML Compliance Officer Responsibilities": "The AML Compliance Officer is also responsible for: ... Reporting to the regulators and auditors on the AML compliance program and its effectiveness; ... Developing and implementing corrective action plans for resolution of problematic issues, and providing general guidance on how to avoid or deal with similar situations in the future."

NEW QUESTION: 15
A □□□ □□ □□□ □□□□ □□□ □□□ B □□□ □□□□□□ □□ □□ □□□ □□□□□. □□ □□□□ A □□□ □□□ □□ □□ □ □□□ □□ □□□ □□ □□ □□□ □□□□□. □□□ □□ □□ □□□□□□□ □□□ 752□ □□□ □□□□□□□. □□ □□□ □□ □□ □□ □□□□ B□□ □□□ □□□□□. 2□ □ □□□□ □□□ □□ □□ □□□□ □□□ □□ 5□ 1□□ □□□ □□□ □□□ □□□□□□□□. □□ □□ □□ □□ □□□ □□□□ □ □□ □□ □□□ □□□□□? (2□□ □□□□□.)
A. □□□□ □□ □□□ □□.
B. □□□□□□ □□□ □□□ □□ □□□□□.
C. □□□□ □□□ □□□ □□□□ □□□□□ □□□ □□□ □□□□□.
D. □□ □□□ □□ □□ □ □□□ □□ □□□ □□ A □□□ □□□□.
E. □□□□□ □□□ 2□ □□ □□□□ □□□□□.
Answer: A,C (LEAVE A REPLY)

According to the Financial Action Task Force (FATF), substantial growth in wealth during a short period of time is a red flag for money laundering or terrorist financing. Additionally, when a client is a family member of a politically exposed person (PEP) from a country known for corruption, it raises concerns about the potential for corruption, bribery, or influence peddling. In this case, the client's father became the president of Country B, which makes him a PEP.

NEW QUESTION: 16

□□ □□□ □□□□ □□ □□□□□□(FIU)□ □□□□□□□□(SAR)□ □□□□ □□ □□□ □□□ □ □□ □ □□ □□ □□□ □□ □□□□?

A. □□ □□□ □□ □□ □□ □□ □□□□ □□□□.

B. 30□ □□□ SAR□ □□□□□□.

C. □□□ □□□□□ □□ □□□□ □□□□□□.

D. □□ □□□□□ □□□□ □□□□ □□ □□□□□□.

Answer: A (LEAVE A REPLY)

The timing of filing a SAR is strictly regulated and depends on jurisdictional laws.

Option A (Correct): Regulatory requirements (e.g., FinCEN in the U.S. mandates filing within 30 days) define the SAR reporting timeline.

Option B (Incorrect): While 30 days is the U.S. standard, other jurisdictions have different deadlines (e.g., EU AMLD mandates "prompt" filing).

Option C (Incorrect): Risk-based assessments are useful, but regulatory deadlines must be followed.

Option D (Incorrect): Subjective decision-making could lead to compliance violations.

NEW QUESTION: 17

□□ □□□ □□□ □□□ □□ □□ □□□ □□ □□□ □□□□□□□? (2□□ □□□□□□.)

A. □□□ □□□□□ □□

B. □□ □□□ □□□□□ □□□□□ □□ □□□□ □□

C. □□□□□ □□□□

D. □□ □□ □□ □□

E. □□ □□

Answer: (SHOW ANSWER)

The practice of brokerage firms maintaining securities as nominees and the speed of the transactions are two factors specific to the securities industry that increase the exposure to money laundering risk. Nominee accounts can be used to conceal beneficial ownership and obscure transaction trails. The speed of transactions can make it difficult to detect and prevent suspicious activity in real time.

NEW QUESTION: 18

□□ □□□ □□ □□□ □□ KYC □□□□□□ □□□□□□ □□ 4□□ □□ □□□ □□□□□□?

A. □□ □□□, □□ □□□□, □□ □□, □□ □□

B. □□ □□, □□ □□, □□ □□, □□□□

C. □□ □□□, □□□ □□□□, □□ □□, □□ □□

D. □□ □□, □□□ □□, □□ □□, □□□□

Answer: (SHOW ANSWER)

According to the Basel Committee on Banking Supervision (BCBS), a sound KYC program should contain four essential elements: (i) customer acceptance policy; (ii) customer identification; (iii) on-going monitoring of higher risk accounts; and (iv) risk management1. These elements correspond to the options B in the question, as customer identification involves verifying the identity and beneficial ownership of the customers, risk assessment involves determining the level of risk posed by the customers and their activities, customer screening involves checking the customers against relevant sanctions and watch lists, and monitoring involves reviewing the customers' transactions and behavior for any anomalies or red flags.

Reference:

Consolidated KYC Risk Management - Bank for International Settlements

NEW QUESTION: 19

□□□ □□ □□□ □□□□ □□□□□□□ □□ □□□ □□□□□. □□□ □□ □□ □ □□□ □□ □□ □□□□□□. □ □□/□□□ □□□□□□ □□ □□□ □□ □□□□□ □□□?

A. □□ □□□

B. □□□ □□□ □□

C. □□ □□

D. □□ □□ □□

Answer: C (LEAVE A REPLY)

When a high volume of incoming wire transfers generates an alert about a client and the funds are immediately debited by cash withdrawals and outgoing wire transfers, the first information that should be reviewed to investigate this alert/case is the customer's account activity. This is because the account activity can reveal the origin, destination, purpose, frequency, and amount of the wire transfers, as well as any unusual or inconsistent patterns that may indicate money laundering or fraud. The account activity can also help to compare the wire transfers with the customer's profile, risk rating, expected behavior, and source of funds. Reviewing the account activity can help to determine if the alert is a false positive or a true positive, and if further investigation or reporting is required.

Reference:

CAMS Study Guide, 6th Edition, Chapter 4, Section 4.3.2, p. 1251

Investigating Alert/Case of High Volume Wire Transfers | CAMS Exam Prep2 Wire Transfer Red Flags: Money Laundering & Fraud Risks - Alessa3

NEW QUESTION: 20
□□ □□ □ □□ □□□ □□□ □□□ □□□ □□□□□?
A. □□□□ □□□□ □□□.
B. □□□□□□□.
C. □□□□□ □□□ □□.
D. □□ □□□□□.
Answer: (SHOW ANSWER)
A politically exposed person (PEP) is a customer who requires the most enhanced due diligence (EDD). This is because PEPs are individuals who hold or have held prominent public positions, such as heads of state, senior politicians, judges, military officers, or directors of state-owned enterprises, and who may pose a higher risk of money laundering, corruption, or bribery due to their influence and access to public funds1. EDD measures for PEPs may include obtaining senior management approval, establishing the source of wealth and funds, and conducting enhanced ongoing monitoring of the business relationship2.
The other customers listed do not necessarily require the most EDD, although they may still present a higher risk of money laundering depending on the circumstances. A resident of a non-cooperative jurisdiction is a customer who lives in a country or territory that has been identified by the Financial Action Task Force (FATF) or other international bodies as having weak or deficient anti-money laundering (AML) standards or posing a threat to the international financial system3. EDD measures for such customers may include obtaining additional information or documentation, applying extra scrutiny to transactions, or refusing to establish or continue the business relationship4. An international business corporation is a customer who operates in multiple jurisdictions and may have complex or opaque ownership structures that can conceal the identity or activity of the beneficial owners or controllers. EDD measures for such customers may include verifying the legal existence and structure of the entity, identifying the beneficial owners and controllers, and understanding the nature and purpose of the business relationship. An established customer is a customer who has a long-standing and regular business relationship with the financial institution and who may have a lower risk of money laundering due to the familiarity and trust that has been built over time. EDD measures for such customers may not be required unless there are changes in the customer's profile, behavior, or risk level.
Reference:
1: Politically Exposed Persons (Recommendations 12 and 22) - FATF1 2: High-risk customers, including politically exposed persons | FCA2 3: High-Risk and Other Monitored Jurisdictions - FATF3 4: Your responsibilities under money laundering supervision | GOV.UK4 : International Business Corporations - ACAMS : Anti-Money Laundering Customer Due Diligence | Veriff.com : Customer Due Diligence - ACAMS : Anti-money laundering - a guide to customer due diligence

NEW QUESTION: 21

□□□ AML □□ □□□ □□□ □ □□ □□□□ □□ □ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□?

A. □□ □□□□ □□ □□□□ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□□ □ □□.

B. □□ □□□□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□□□.

C. □□ □□□ □□ □□□ □□ □□□ □□□□□ □□□□ □□□□□□□.

D. □□□ □□□□□ □□□ □□ □□□ □□□□ □□□□ □□□□□.

Answer: B,C (LEAVE A REPLY)

AML compliance must be balanced with data protection laws such as GDPR (EU), CCPA (U.S.), and local banking secrecy laws.

Option B (Correct): Data minimization ensures financial institutions only collect and retain essential customer data needed for AML compliance.

Option C (Correct): Regularly updating data processing policies ensures compliance with evolving data protection regulations.

Why Other Options Are Incorrect:

Option A (Incorrect): Unrestricted access to customer data increases privacy risks and can violate GDPR and other data protection laws.

Option D (Incorrect): AML data must not be repurposed without regulatory justification, as GDPR requires data usage to align with its original collection purpose.

Best Practices for Managing Data Privacy in AML Compliance:

Restrict access to AML data on a need-to-know basis.

Implement strong encryption and security controls for customer data.

Ensure all AML-related data collection aligns with privacy regulations.

Reference:

General Data Protection Regulation (GDPR), Article 5 (Principles for Data Processing) FATF Recommendation 2 (National AML Cooperation & Data Sharing)

6th EU AML Directive (6AMLD) on Data Protection and AML Compliance

NEW QUESTION: 22

□□□□□□(FATF) □□□ □□ □□□ □□□□ □□ □□□□□ □□□□□□□ □□□□ □ □ □□ □□□ □□□?

A. FATF □□ □□□ □□□□ □ □□ □□□□□ □□ □□□ □□□□□.

B. FATF □□ □ □□ □□□ □□□□ □□□ □□ □□□ □□□□□ □□□□□ □□□□□.

C. □□□ □□□□□□ □ □□□□□□□□ □□□ □□□□□ □□ □□□□ □□□□□.

D. □□□□ □□□□□ □□□□□□ □ □□□□□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

financing

Explanation:

. Financial Action Task Force (FATF)-style regional bodies (FSRBs) are organizations that associate countries from the same region or that face similar challenges to combat money laundering and terrorist financing. FSRBs have the same objectives as the FATF, which are to set

international standards and promote effective implementation of legal, regulatory and operational measures to prevent and combat money laundering and terrorist financing. One of the main functions of FSRBs is to provide technical assistance and training to their members in implementing the FATF recommendations, which are the global standards for anti-money laundering and counter-terrorist financing. FSRBs also conduct mutual evaluations of their members to assess their level of compliance with the FATF recommendations and provide follow-up reports and actions.
Reference:
CAMS Study Guide, 6th Edition, Chapter 2, Section 2.11
Certification Candidate Handbook, Section 3.22
FATF website, About Us, FATF-Style Regional Bodies3

NEW QUESTION: 23
□□ □□□(USA PATRIOT ACT)□ □□ □□ □ □□ □ □□□ □□ □□ □□□ □□ □ □□□ □ □□ □□□□□□? (3□□ □□□□□□.)
A. □□ □□□□□□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□ □ □□ □□□ □ □□□□.
B. □□ □□□ □□□□□□ □□□ □□□ □□□□ □□□□ □□□ □□□□ □□ □ □□□ □ □□.
C. □□ □□□ □□□□ □□□ □□□□ □□ □□ □□ □□□ □□ □□ □□(FI)□ □□ □□ □ □□□□□□ □□□ □ □□□□.
D. □□□ □□ □□□ □□□ □□ □□·□□□□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□□□ □□.
E. □□□-□□, □□□ □ □□□□ □□□□ □□ FI □□□ □□□□□.
F. □□ □□ □□□□ □□□□ □□□□ FI□ □□ □□ □□□□ □□ □□□ □□□ □ □□□ □.
Answer: (SHOW ANSWER)
The USA PATRIOT Act is a comprehensive legislation that was enacted in response to the terrorist attacks of September 11, 2001, and aimed to strengthen the US government's ability to prevent, detect, and prosecute money laundering and terrorist financing. Among its many provisions, the USA PATRIOT Act contains several sections that have extraterritorial reach, meaning that they apply to foreign entities or activities that have a nexus with the US. Three of these sections are:
Section 319(b), which allows for the US Attorney General or the Secretary of the Treasury to issue a subpoena or other legal order to any foreign bank that maintains a correspondent account in the US, requiring the production of records relating to such account or any account at the foreign bank, including records maintained outside the US12. This section also allows foreign banks to voluntarily designate a registered agent in the US to accept service of such subpoenas or orders12.
Section 313, which prohibits US financial institutions from establishing, maintaining, administering, or managing correspondent accounts for foreign shell banks, which are banks that

have no physical presence in any country and are not affiliated with a regulated financial group34. This section also requires US financial institutions to take reasonable steps to ensure that their correspondent accounts with foreign banks are not being used to provide banking services indirectly to foreign shell banks34.
Section 311, which authorizes the Secretary of the Treasury to designate foreign jurisdictions, financial institutions, classes of transactions, or types of accounts as being of "primary money laundering concern" and to impose special measures to address such concerns . These special measures may include requiring US financial institutions to obtain and retain information on the beneficial owners of foreign accounts, prohibiting or imposing conditions on the opening or maintaining of correspondent or payable-through accounts for foreign financial institutions, or requiring US financial institutions to identify the customers of their foreign correspondent account holders . The Secretary of the Treasury may also order a US financial institution to terminate a correspondent account within 10 days if the foreign bank fails to comply with a subpoena or other request for information under Section 319(b) .
Reference:
1: USA PATRIOT Act, Section 319(b)
2: ACAMS, CAMS Certification Package - 6th Edition, Chapter 4, page 121
3: USA PATRIOT Act, Section 313
4: ACAMS, CAMS Certification Package - 6th Edition, Chapter 4, page 120
: USA PATRIOT Act, Section 311
: ACAMS, CAMS Certification Package - 6th Edition, Chapter 4, page 119
https://www.jonesday.com/-/media/files/publications/2007/10/extraterritorial-application-of-the-usa-patriot-ac/files/extraterritorial-application-of-the-usa-patriot-ac/fileattachment/graves_ganguli.pdf
https://www.lawfareblog.com/long-arm-us-law-patriot-act-anti-money-laundering-act-2020-and-foreign-banks

NEW QUESTION: 24
□□ □□ □□ □□ □□ □□ □□□□□□□ □□□ □ □□ □□□ □□□□□□?
A. □□□□□ □□ □□ □□□ □□□ □□□ □ □□□□.
B. □□□ □□□□□□ □□□ □□□□□□ □□□□□ □□□.
C. □□ □□□ □□□□□ □□□ □□ □□□ □□□□□ □□□ □□ □□ □□□□□□□ □□□ □ □□□.
D. □□□ □□ □□ □□□ □□ □□□ □□□ □ □□□ □□□□□ □□ □□□ □□ □□□□□□ □□□□.
Answer: B (LEAVE A REPLY)
The first valid step in the Mutual Legal Assistance Treaty (MLAT) international cooperation process is for the central authority of the requesting country to send a letter of request to the central authority of the other country. The letter of request should provide a summary of the facts and information required, the reasons for the request, and any specific legal or procedural requirements that need to be met. (CAMS Manual, 6th Edition, Page 233).

NEW QUESTION: 25
AML □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□ □□□□ □ □ □□ □□□□.
A. □□□ AML □□ □□□□□ □□□□ □□□ □□□ □□□□□□□ □□□ □ □□ □□ □ □□ □□□□.
B. □□□ □□□□□ □□ □□ □□□ □□□□ □□□ □□□□ □ □□□□ □□□ □ □□ □ □ □□□ □□□□.
C. □□□ AML □□ □□□□□ □□□□ □□□ □□□ □□ □□□ □□□□ □□□ □ □□ □ □□ □□
D. □□□ □□ □□ □□ □□□□□ □□□□ □□□ □□□ □□ □□□□□ □□□ □ □□ □ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
□□ □□ □□ □□□□ □□ □□□□ □□□□□ □□ □□□ □□□ □□ □□□□□ □□□ □. □□ □□ □ □□ □□□ □□?
A. □□□ □□ □□□ □□ □□ □□□ □□□ □ □□□ □□□.
B. □□ □□ □□□□ □□□□ □□ □□□ □□□□□ □□□ □□□□□.
C. □□ □□ □□□□ □□□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
A significant reduction in suspicious transaction report (STR) filings at a particular branch could indicate that the branch is not properly identifying and reporting suspicious activities, or that the branch is experiencing a change in customer behavior or risk profile. Therefore, the most appropriate action for an anti-money laundering specialist is to review the branch exception reports, which are reports that highlight transactions or activities that deviate from the expected or normal patterns, based on the customer profiles and risk assessments. By reviewing the branch exception reports, the specialist can determine whether there are any changes in activity that warrant further investigation or reporting, or whether there are any gaps or weaknesses in the branch's compliance program or procedures.
The other options are not as appropriate as reviewing the branch exception reports, as they do not directly address the issue of suspicious activity reporting. Placing the branch on the watchlist may be a subsequent action, but it does not provide immediate insight into the reason for the reduction in STR filings. Analyzing the branch activity reports may show whether there has been a decrease in branch activity, but it does not explain why the activity has decreased, or whether the remaining activity is suspicious or not. Reviewing the staff records may reveal whether inexperienced personnel are in critical positions without appropriate training, but it does not account for other factors that may affect the branch's compliance performance, such as management oversight, internal controls, or customer risk.

NEW QUESTION: 27

□□ □□□ □□□ □□ □□□ □□□ □□□□□□□. □□ □□□ □□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□. □ □□□ □□ □□ □□□□ □□ □□□□□□□. □□□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□ □□ □□□ □□□□□□. □□ □ □□□□ □□ □□□□ □□□ □□□□ □ □□ □□□□□?

A. □□ □□□□ □□□□ □□□□ □□□□ □□□□□ □□□ □□□□□.

B. □□□□ □□□ □□□ □□□□ □□ □□□ □□ □□ □ □□ □□□ □□□□.

C. □□□□□ □□ □□□□ □□□□ □□ □□□□□ □□□ □□□□□□□.

D. □□ □□□ □□□ □□ □□□□ □□ □□ □□□ □□ □□□□ □□□□□.

Answer: C (LEAVE A REPLY)

According to the Anti-Money Laundering Specialist (the 6th edition) resources, one of the red flags for money laundering in real estate transactions is the use of an appraiser who is not on the approved list of the financial institution. This could indicate a possible collusion between the appraiser and the borrower or the underwriter to inflate the value of the property and obtain a higher loan amount. The anti-money laundering specialist should document the underwriter's actions and the reasons for approving the exception, as well as the discrepancy between the appraised value and the market value of the property. The specialist should then file a suspicious transaction report (STR) to the relevant authorities, as required by the local regulations .

Reference:

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 7: Money Laundering Risks and Methods, page 201.

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 8: Anti-Money Laundering Programs, page 227.

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 9: Conducting or Supporting the Investigation Process, page 255.

NEW QUESTION: 28

5□ EU □□ □□ □□□ □□□ □□□□ □□□ □□□ □3□ □□□ □□□ □□□□ □□ □ □ □□□ □□□□ □□□ □□ □□ □□□ □□□ □□ □□□□□. □□□ □□ □□□□ □□ □□ □□□□□? (3□□ □□□□□.)

A. □□□□ □□□ □□ □□ □□□ □□ □□ □□□□ □□□ □□ □

B. □□ □□□ □□ □□□ □□ □□ □□

C. □□□□□ □□ □□ □ □□

D. □□□ □□□□□ □□□ □□□ □□ □□ □□

E. □□□□□□ □□ □□ □□ □□ □□ □□

F. □□ □ □□□ □□□□ □□ □□ □ □□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

these are the enhanced customer due diligence measures that the 5th EU Money Laundering Directive requires for high-risk third country nationals. According to the directive, entities must obtain the approval of senior management for establishing or continuing the business

relationship, obtain information on the reasons for intended or performed transactions, and obtain information on the source of funds and source of wealth of the customer and of the beneficial owner(s). These measures are intended to increase the transparency and scrutiny of the customers and their transactions, and to prevent the misuse of the financial system for money laundering or terrorist financing purposes.
Reference:
ACAMS Study Guide 6th Edition, Chapter 2, Section 2.3, page 56: "The EU's Fifth Anti-Money Laundering Directive".
ExamTopics, Question 456: "According to the 5th EU Money Laundering Directive, member states require entities to apply enhanced customer due diligence measures with respect to business relationships or transactions involving high-risk third country nationals. Which are included in these requirements? (Choose three.)"

NEW QUESTION: 29
□ □□ FIU(Financial Intelligence Unit)□ □□ □□□ □□□□ Egmont Group□ □□□ □□□ □□?
A. □□□□□ □ □□□□□□□ □□□ □□ □□□□□ □□□□□ □□ □□□□□□ □□□ □□□□□ □.
B. □□□□□ □ □□□□□□□□□ □□□□□ □□□□ □□□□□ □ □□□□□ □□ □□□□□□ □□□ □□□□□ □□ FIU□ □□ □□□ □□□□□□.
C. □□□□□ □ □□□□□□□□□ □□□□□ □ □□□□□□□ □□□□□□ □□□□□ □ □□□□□ □ □ □□□□□□ □□□ □□□□□□.
D. □□□□□ □ □□□□□□□ □□□ □□ □□□ □ □□□□□□□ □□□ □□□□□ □ □□□ □ □ □□□□□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
According to the web search results, the Egmont Group is a united body of 170 Financial Intelligence Units (FIUs) that provides a platform for FIUs to securely exchange expertise and financial intelligence to combat money laundering, terrorist financing, and associated predicate offences12. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing, and other financial crimes345. The other options are not correct because they either do not capture the full scope of the Egmont Group's activities, or they are not the primary focus of the Egmont Group.
Reference:
https://2009-2017.state.gov/j/inl/rls/nrcrpt/2015/vol2/239473.htm\

NEW QUESTION: 30
□□ CEO□ □□ □□□ □□□□ □□ □□□ □□ CEO□ □□□ □□□ □□□ □□ □□ CEO□ □□□ □□ □□□ □□□ □□□?
A. □□□ □□□□ □□□ □□□□□.
B. □□ □□□ □□ □□□ □□□□□ □□□ □□□□□.

C. □□ CEO□ □□□□□□ □□□ □□□□□□.

D. □□ □□ □□ □□ □□□□□ □□□□□ □□ □□□ □□□□□□.

Answer: D (LEAVE A REPLY)

Submitting the concern anonymously to the bank's internal Compliance Hotline is the most appropriate action that a bank CEO's assistant should take when the bank CEO expenses large sums of money to a charitable organization run by the bank CEO's direct family member. This is because this action would allow the assistant to report a potential case of fraud, conflict of interest, or misuse of funds without fear of retaliation or reprisal from the bank CEO. The Compliance Hotline is a confidential and secure channel for employees to raise any concerns or suspicions about unethical or illegal activities within the bank. The Compliance Hotline would then forward the concern to the relevant authorities or departments for further investigation and action.

Reference:

The document titled "Anti-Fraud Policy" published by the World Bank Group. You can access it by clicking here. This document states that "The World Bank Group has established a Compliance Hotline to receive reports of suspected fraud or corruption in World Bank Group-financed projects or activities, or in the World Bank Group's corporate procurement or administrative activities. The Compliance Hotline is available to all staff and external parties, such as contractors, consultants, beneficiaries of World Bank Group-financed projects, and the general public.

NEW QUESTION: 31

□□ □□ □□ □□□ □□ Wolfsberg Group□ □□□□□ □□ □□ □□ □□□□□ □□□ CTF □ □□ □□□□□□ □ □□ □□□ □□□□□□?

A. □□ □□□ □□□□□ □□ □□□ □□□ □□□□□□ □□□□□ □□ □□□ □□□ □□□□□.

B. □□□ □□ □□□□□ □□□□□□ □□□□□ □□ □□□ □□ □□

C. □□ □□□ □□□ □□□ □ □□□ □□ □□

D. □□□□□ □ □□□ □□□ □□

Answer: A,B,C (LEAVE A REPLY)

According to the Wolfsberg Group's Statement on the Suppression of the Financing of Terrorism1, a compliance officer should include the following three procedures in revising an institution's CTF efforts:

Consulting applicable lists and taking appropriate actions to determine if customers appear on such lists. This procedure is important to prevent terrorist organizations from accessing the financial services of the institution and to comply with the sanctions and regulations imposed by competent authorities. The compliance officer should implement procedures for checking the customers against the lists of known or suspected terrorists or terrorist organizations issued by relevant authorities and taking reasonable and practicable steps to verify the identity and status of the customers.

Reporting matches from lists of known or suspected terrorists to relevant authorities. This procedure is important to assist the authorities in their efforts to detect and disrupt terrorist financing and to fulfill the legal obligations of the institution. The compliance officer should report to the relevant authorities any matches from the lists of known or suspected terrorists or terrorist

organizations consistent with the applicable laws and regulations regarding the disclosure of customer information.
Maintaining customer information to facilitate timely retrieval of such information. This procedure is important to enable the institution to respond promptly and effectively to the enquiries and requests from the authorities and to enhance the quality and accuracy of the customer data. The compliance officer should explore ways of improving the maintenance of customer information to facilitate the timely retrieval of such information.
Reference:
Wolfsberg Statement on Anti-Terrorism Financing
UNUSUAL CUSTOMER IDENTIFICATION CIRCUMSTANCES
* Customer furnishes unusual or suspicious identification documents or declines to produce originals for verification."

NEW QUESTION: 32
□□□□□□ □□□ □□□ □□□□□□?
A. □□□□□□ □□ □ □□□□□ □□□□□ □□ □□
B. 20□□, 10□□□ □□□□□ □□□□□ □□□□□□ □□□□□ □□□
C. □□□□□□ □□□□□□ □□ □□□□□ □□□□ □□□□□ □□
D. □□□ □□□□□ □□ □□ □3□ □□ □□□□□□ □□□□□ □□□□ □□□□□
Answer: (SHOW ANSWER)
Large and frequent credit balances on a credit card resulting in request for refunds is an indicator of suspicious activity because it may suggest that the cardholder is using the credit card to launder money or to conceal the source of funds. This is also known as credit card refund fraud or credit card laundering. The cardholder may make purchases with the credit card using illicit funds, then request refunds to another account or in cash, thus transferring the funds to a legitimate or less traceable channel. This activity may also be used to evade currency reporting requirements or to avoid detection by law enforcement or financial institutions.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 2: Money Laundering Risks and Methods, page 381 Suspicious Activity Reporting Indicators and Examples, U.S. Department of Homeland Security, Indicator 14: Excess Purchases or Transactions2 Credit Card Laundering, Money Laundering Bulletin, Issue 245, October 2019

NEW QUESTION: 33

□□ □□□□□□□□□ □ □□ □□ □□□ □□□□□□?

A. □□□, □□, □□□□

B. □□, □□, □□

C. □□, □□, □□

D. □□, □□, □□

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

A National Financial Intelligence Unit (FIU) has three primary functions: receiving, analyzing, and disseminating information related to suspicious financial activities. The FIU's main focus is to identify and investigate suspicious activities, such as money laundering, terrorist financing, and other financial crimes. The FIU also works with other organizations and agencies to develop effective and efficient financial crime prevention strategies. The FIU is tasked with developing an effective system for receiving, analyzing, and disseminating information related to suspicious financial activities. The information collected is then used to identify, investigate, and prosecute financial crimes.

NEW QUESTION: 34

□□□□□□ □□□ □□ □□□ □□ □□□□□□ □□□□ □□□? 3□□ □□□ □□□□□□

A. □□□ □□□ □□□□ □□□ □□□□□□.

B. FATF □□□□□□□ □□ □□□ □□ □□

C. □□□ □□□□ □□

D. □□□□ □□ □□

Answer: ([SHOW ANSWER](#))

One of the key components of an effective anti-money laundering (AML) program is to implement adequate customer due diligence (CDD) measures for new accounts. This includes verifying the identity of the party opening the account, determining the beneficial owner(s) of the account, and seeking to determine the source of deposited funds. These measures help the financial institution (FI) to understand the nature and purpose of the customer relationship, assess the risk profile of the customer, and detect and report any suspicious or unusual activity. Documenting the identity of the party opening the account and the beneficial owner(s) of the account also helps the FI to comply with the record-keeping and reporting requirements of the AML laws and regulations, and to cooperate with the authorities in case of investigations or inquiries. Seeking to determine the source of deposited funds helps the FI to prevent the introduction of illicit funds into the financial system, and to identify any discrepancies or inconsistencies between the customer's profile and activity.

Reference:

1: FATF Guidance for a Risk-Based Approach for the Banking Sector1

2: OCC Bulletin 2020-10: Customer Due Diligence and Bank Secrecy Act/Anti-Money Laundering Examination Procedures2

3: ACAMS Study Guide for the CAMS Certification Examination3

NEW QUESTION: 35

□□□ □□ □□ □□□ □□□□□□□ □□ □□□ □□ □□ □□□□□ □□□ □□ □□ □□□ □ □□□□□□□.

□ □□□□ □□□ □□□ □□ □□□ □□ □□ □□□ □□□ □□□?

A. □□□ □□□ □□□ □□□ □□□□□□.

B. □□□ □□ □□ □ □□□ □□ □ □□ □□ □□

C. □□□□ □□□ □□ □□□ □□□□ □□□ □□□□.

D. □□ □□□□□□□ □□□ □□□ □□□□ □□ □ □□□ □□□ □□

Answer: B (LEAVE A REPLY)

According to the CDD Rule, covered financial institutions must establish and maintain written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers and to include such procedures in their anti-money laundering compliance program1. These procedures should also be updated as necessary to reflect changes in the law or the institution's risk profile2. Moreover, the institution should provide adequate training to its employees on the new requirements and monitor their compliance3.

Reference:

1: FinCEN Guidance, FIN-2020-G002, August 3, 2020, p. 1

2: Your responsibilities under money laundering supervision - GOV.UK, Section: Customer due diligence requirements

3: Customer identification: Know your customer (KYC) | AUSTRAC, Section: Training and awareness

NEW QUESTION: 36

FinCEN□ □□□, □□ □□ □□ □□ □□ □□□ □□□ □□ □□, □□□□, □□□ □□□ □ □□□□? (□ □□□ □□□□□.)

A. □□□ □□□□ □□□□□□□ □□ □□.

B. □□□ □□□ □□ □ □□ □□□ □□ □□□ □□.

C. □□□ □□□ □□□ □3□ □□ □□□□□□□□ □□□□ □□ □□□□□.

D. □□ □□ □□□□□□ □□□ □□ □□.

Answer: B,C (LEAVE A REPLY)

Human trafficking and modern slavery involve illicit financial transactions, often conducted through banks, money service businesses (MSBs), or virtual assets.

Option B (Correct): Frequent payments for online advertisements can indicate recruitment for illicit labor or trafficking operations.

Option C (Correct): Incoming funds from third-party processors with unclear originators suggest concealed financial flows linked to illicit activities.

Why Other Options Are Incorrect:

Option A (Incorrect): Transactional activity with a virtual currency exchange alone is not a strong human trafficking red flag.

Option D (Incorrect): Cash payments to workers could indicate labor law violations but do not necessarily indicate human trafficking.

Common Financial Red Flags for Human Trafficking:
Unexplained cash deposits and withdrawals from multiple accounts.
Frequent wire transfers to high-risk jurisdictions.
Use of prepaid cards to move funds anonymously.
Best Practices for Detecting & Preventing Human Trafficking-Related Transactions:
Train frontline staff to recognize financial indicators of trafficking.
Monitor unusual transaction patterns in industries with high labor exploitation risks.
File Suspicious Activity Reports (SARs) when trafficking-related transactions are suspected.
Reference:
FinCEN Human Trafficking Financial Red Flags (2021)
FATF Report on Financial Flows Linked to Human Trafficking
6th EU AML Directive (6AMLD) on Human Trafficking & Financial Crime

NEW QUESTION: 37
□□□□□□□ □□□□□□ □□□□□ □□ □□□□□□ □□□ □ □□ □□□ □□□□□□?
A. □□□□□ □□ □□□ □□□□□ □□□.
B. □□ □□ □□□ □□□ □□□□□□ □ □□□□□□□ □□□□□ □□□.
C. □□□ □□□ □□□□□ AML □□□□□□ □□□ □□□ □□□□□ □□□.
D. □□ □□□ □□ □□ □□□ □□ □□ AML □□□ □□□□□ □□ □□□.
Answer: A ([LEAVE A REPLY]())
A comprehensive risk analysis is the first and most important step in developing an effective anti-money laundering program. A risk analysis helps a financial institution identify and assess its exposure to money laundering and terrorist financing risks, based on its products, services, customers, geographic locations, and other factors. A risk analysis also enables a financial institution to tailor its policies, procedures, controls, and training to mitigate the specific risks it faces. A risk analysis should be conducted periodically and updated as necessary to reflect changes in the institution's risk profile.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 2: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Section 2.1: Risk-Based Approach, p. 29-30 ACAMS Risk Assessment, What is Anti-Money Laundering (AML) Risk Assessment?
How to Conduct an AML Risk Assessment - Assess Key Risk Drivers

NEW QUESTION: 38
□□□ □□□□□□□ □□□ □□□ □□□□□ □□□□□ □□□ □□□ □□□ □□□□□.
□ □□□ □□ □□ □□□□□ □□□□□ □ □ □□ □□□ □□□□□□? (2□□ □□□□□□.)
A. □□□ □□□ □□ □□□ □□□ □□□□□.
B. □□ □□ □□ □□ □□ □□□ □□ □□
C. □□□ □□□□□□ □□□□□ □□ □□ □□ □□□ □□ □□□ □□□□□ □□□□□.
D. □□□ □□□ □□ □□□ □□□□□ □□□□□□ □□ □□□ □□□□.

Answer: C,D (LEAVE A REPLY)

The customer's wire transfers to high-risk jurisdictions and the large volume of activity with low month-end balance are two facts that should be considered during the course of an investigation into possible money laundering. These facts may indicate that the customer is trying to move funds from or to countries that have weak anti-money laundering (AML) controls, or that are known to be a source or destination of illicit funds12. They may also suggest that the customer is using a technique called "smurfing" or "structuring", which involves breaking down large amounts of cash into smaller transactions to avoid detection or reporting34. The other two facts are not necessarily indicative of money laundering, as the customer may have a legitimate reason to have a long-standing account at the bank or to be on the exempt list for currency transaction reporting requirements.

NEW QUESTION: 39

□□ □□□ □□□ 55,518 USD□ □□□□□□□. □□□ □□ □□□ □□□□ □□ □□□ □□ □ □□□□□ □□□□□□. □□ ^□□□ □□□□□ □□□□□□? (2□□ □□□□□□.)

A. □□□ □□ □□ □□ □□ □□ □□ □□ □□□ 100,000 USD□ □□□□,

B. □□□ 10,000 USD □□□ □□□ □□□ □□□□□□□ □□□□□.

C. □□□ □□ □□□ □□□ □□ □□ □□ □□ □□ □□ □□ □□□ □□□□□.

D. □□□ □□□□ □ □□ □□□ □□□□□□□ □□□□□.

E. □□□ □□□ □□ □□□ □□ □□ □□ □□ □□□ 50.000 USD□ □□□□□.

Answer: (SHOW ANSWER)

These options involve transferring funds to another country, which could indicate cross-border movement of illicit funds, and cashing out winnings in checks under 10,000 USD, which could indicate structuring to avoid reporting thresholds. The other options do not seem as suspicious or relevant to money laundering.

NEW QUESTION: 40

□□□□□□□ □□ □□ □ □□□ □□□ □□□□.

A. □□□□□ □□□ □□□ □□□ □□□□□.

B. □□□□□ □□ □□ □ □□ □□□ □□□ ATM □□.

C. □□ □□ □□ □□□ □□ □□.

D. □□□ □□ □□□ □□ □□ □□□□□.

Answer: D (LEAVE A REPLY)

Microstructuring is a method of money laundering that involves breaking down large transactions into smaller amounts that are below the reporting threshold or the level of scrutiny of financial institutions. One of the red flags of microstructuring is frequent visits to make cash deposits of nominal amounts, as this may indicate an attempt to avoid detection and conceal the source or destination of illicit funds. Other red flags of microstructuring include checking accounts receiving cash deposits in amounts under $1,000 as infrequently as several times a month, followed by ATM withdrawals in foreign countries, or deposits that are inconsistent with the customer's profile or business activity.

Reference:
FinCEN Advisory - FIN-2010-A001, page 4
Red Flags of Money Laundering | PPT, slide 9
Red Flags of Microstructuring | CAMS Exam Preparation | ACAMS

NEW QUESTION: 41
□□ □□□ □□□□□□□ □□ □□□□□□□ □□ □□□ □□ □□ □□ □□□ □□ □□ □□
□□□(OFAC>□ □□□ □□ □□□ □□□□□ □□□ □□□□□ □□□□□ □□□ □□□□. □□
□□ □ □□ □□ □□□ □□□ □□□ □□ □□□□□ □□ □□?(2□ □□)
A. □□□ □□□□□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□.
B. □□ □□□ OFAC□ □□□ □□ □□□ □□□□□ □□□ □□□□□ □□ □□□ □□□ □□
□ □□□□(USA PATRIOT Act □□□□).
C. USA PATRIOT Act□ □□□ □□ □□ □□□□□□ □□ □□□ □□ □□□ □□□□□ □□ □
□□ □□□ □□□ □ □□ □□□ □□□□□.
D. □□ □□□ OFAC □□ □□□ □□□□□□□ □□□□□□□ □□□ □□ □□ □□□ □□□
□□ □□□ □□ □□ □□□ □□ □ □□□□.
E. □□ □□□ □□□ UN□ □□□ □□ □□□ □□ □□□□ OFAC □□□ □□ □□ □□□
□□□ □□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)
According to the USA PATRIOT Act, US authorities do have the power to subpoena records from foreign banks that maintain correspondent accounts with US banks. This is known as a "section 314(a) request," which allows law enforcement to obtain information related to suspected terrorist financing or money laundering.
However, US authorities are not limited to seizing only funds transferred under OFAC sanctions if there is an equivalent UN sanctions regime that has been contravened. The US government can impose its own sanctions that are independent of the UN, and can seize funds or take other actions to enforce those sanctions.
Therefore, the correct answers to the question are A and C:
A . If the funds are seized, then the foreign bank would be within its rights to dispute such seizure.
C. The USA PATRIOT Act authorizes the Secretary of the Treasury or the Attorney General to subpoena records from the foreign bank that maintains a correspondent account with a US bank.

NEW QUESTION: 42
□□□ □□□□□ □□□□ □□□□□□□ □□□ □□□□□□□. □□ □□ □□□ □□□□ □
□ □□ □□□□ □□ □□□□ □□□□□. □□ □□ □□ □□ □□□ □□ □□□ □□□□□
□. □□ □□□□□ □□ □□□ □□□ □□ □□ □□ □□□ □□□ □ □□□□□. □□ □□
□ □□ □□□ □□□ □□□ □□□ □□□□□□□. □□ □ □□ □□□ □□ □□ □□□□ □
□ □□ □□□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□□□ □□□□ □□□□□□ □□□□.
B. □□□□□ □□□ □□□ □□□ □□□□□□ □□ □□□ □□ □□□ □□□□□.
C. □□□ □□□□ □□□ □□ □□□ □□□□□.

D. □□□ □□ □□□ □□ □□□□□ □□(□□)□ □□ □□□ □□□□□□.

Answer: B (LEAVE A REPLY)

According to the Basel Committee on Banking Supervision's Customer Due Diligence for Banks1, banks should have policies and procedures to identify and manage high-risk customers, such as those who provide false or incomplete information, have complex or opaque beneficial ownership structures, or are involved in large or unusual transactions. In such cases, banks should apply enhanced due diligence measures, such as obtaining additional information or documentation, verifying the source and purpose of funds, conducting more frequent and intensive monitoring of account activity, and reporting any suspicious transactions to the relevant authorities. Therefore, the best course of action for the bank in this scenario is to implement enhanced due diligence procedures to monitor the account for suspicious activity, as option B suggests. Option A is not recommended, as it would imply that the bank accepts the customer without verifying his identity and background, which would expose the bank to money laundering and terrorist financing risks. Option C is not advisable, as it would terminate the relationship without investigating the origin and destination of the funds, which could hinder the efforts of law enforcement agencies to trace and recover illicit assets. Option D is also not appropriate, as it would involve sending a check to a customer whose address and identity are not confirmed, which could facilitate money laundering and fraud.

Reference:

5: Customer due diligence for banks - Bank for International Settlements, October 2001, pages 8-9, 13-14.

NEW QUESTION: 43

□□ □□□ □□□□□□ □□□ □□□ □ □□ □□□ □□□ □□ □□□ □□□ □□□ □□ □ □□ □□ □□□□□ □□ □□?

A. □□□ □□□ □□□ □□ □ □□ □□□ □□ □□□ □□□ □□□□□ □□□ □□□□□ □□ □□ □ □□□□□.

B. □□□□□ □□□ □□□ □□□□□ □□□ □□ □□ □□□□□ □ □□□, □□□ □□ □□ □□ □ □□□ □□ □□□ □□□□□□.

C. □□□ □□□□□ □ □ □□ □□ □□, □□□ □□□□□ □□□□□ □□□ □□□ □□□ □□□ □□ □□ □□□ □□ □□□□□ □□□.

D. □□□□□ □□□□□□ □□□□□ □ □□ □□□ □□□ □□ □□□ □□ □□□ □□□, □□□ □ □□□□□ □□□□□ □□□ □□□ □ □□□.

Answer: B (LEAVE A REPLY)

According to the CAMS Study Guide, page 173, "If an independent investigation provides grounds to interview the employee, the employee can be interviewed and, if necessary, terminated, but not advised that he or she is under investigation by law enforcement." This is because informing the employee of the law enforcement investigation could compromise the integrity of the case and potentially expose the institution to legal liability. Therefore, option B is the correct answer.

Reference:

CAMS Study Guide, page 1731
CAMS Exam Questions and Free Practice Test, Question 2872

NEW QUESTION: 44
□□□ □□ □□□□□ □□□ □□ □□ □□ □□□□□□ □□□□□ □□ □□□ 6□□ □□ □□□ □□□ □□□□. □ □□□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□□ □□ □□ □□ □□□ □□□□□□□□.
□□ □□ □□□□□ □□□ □□ □□□ □□□□□□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□
B. □□ □□□ □□□ □□□ □□□□□□□□.
C. □□ □□ □□□ □□□□□□□□□.
D. □□ □□□ 6□□ □□ □□□
Answer: A (LEAVE A REPLY)
Assessing AML/CFT is an ongoing and evolving component of maintaining a compliant AML/CFT program. Evaluating the risk-scoring model and conducting the risk assessment itself may need to be performed annually, every 18 to 24 months, before the launch of a new product or when an acquisition of another financial institution occurs.

NEW QUESTION: 45
□ □□ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□□.
A. □□□□ □□□ □ □□□ □□ □□□ □□□□□□□.
B. □□□-□□□ □□□ □□ □□□□ □□□ □□□□□.
C. □□□ □□□ □□ □□
D. □□□ □□□ □□□□ □□ □□ □□ □□□ □□
Answer: D (LEAVE A REPLY)
Financial institutions are required by law to maintain records and documentation of customer transactions and to provide this information to law enforcement agencies upon request. However, financial institutions should also have policies and procedures in place to ensure that they comply with legal and regulatory requirements and protect customer privacy. Providing protected documents that are privileged under attorney-client privilege or freezing an account immediately may not be the appropriate response and may expose the financial institution to legal or reputational risks.

NEW QUESTION: 46
□□ □□□ □□□□ □ □□ □□□□□□□□ □□□□ □□ □□□ □□□ □□□□□ □□□□ □□□□□. □□ □□□ □□□ □□ □ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□ □ □□□□ □□□ □□□ □□ □□□ □□□□□□□.
□□ □□ □□□ □□□ □□ □□ □□□ □□□□□?
A. □□□□ PEP(□□□ □□□)□□ □□□ □□ □□□□□ □□□.
B. □□□□□ □□□□□ □□□ □□

C. □□□□□□ □□ □□□□□ □□□□□□ □□□□ □□ □□ □□ □□□ □□□ □□□ □□□ □.
D. □□□□□□ □□□ □□□□□ □□□ □□□□□□ □□
Answer: D (LEAVE A REPLY)
A key risk indicator associated with terrorism financing is the link between the charity group and a known terrorist group. This indicates that the funds transferred to the charity group may be used to support the terrorist group's activities, such as recruitment, training, propaganda, or attacks.
Charities are often vulnerable to abuse by terrorist financiers, as they may operate in high-risk areas, have access to large amounts of cash, and enjoy public trust and legitimacy. Therefore, financial institutions (FIs) should conduct due diligence on the charity group, its directors, its beneficiaries, and its sources and uses of funds, and monitor the transactions for any red flags, such as unusual patterns, amounts, or destinations. FIs should also comply with the relevant sanctions and regulatory requirements, and report any suspicious or unusual activity to the authorities.
Reference:
1: FATF Guidance on Private Sector Information Sharing1
2: Mitigating the risks of terrorist financing | Crowe LLP3
3: ACAMS Study Guide for the CAMS Certification Examination3

NEW QUESTION: 47
□□□□□ □□ □□□□□□ □□ □□□ □□□ □ □ □□ □□□□□□ □□□ □□□□□□?
A. □□ □□□ □□□□□ □□ □□ □□□ □□ □□□□□ □□□ □□□□□□.
B. □□□ □□□ □□□ □□□□□ □□ □ □□□□□ □□□ □□□□□.
C. □□□ □□□ □□□□□□ □□□ □□□□□ □□□ □□ □□□□□□.
D. □□□ □□□□□ □□□ □□□ □□ □□ □□□□□□ □□□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
Casinos are high-risk for money laundering due to their cash-intensive nature and ease of moving funds anonymously.
Option A (Correct): A private company sending funds into multiple patron accounts is suspicious because it may indicate money laundering structuring or use of mules.
Option B (Incorrect): Betting on multiple events is normal behavior unless there is evidence of match-fixing.

Option C (Incorrect): Large cash buy-ins are common in casinos; however, they become suspicious when coupled with other red flags (e.g., no actual gambling).
Option D (Incorrect): Transferring winnings may be a regular transaction unless linked to structured transactions.

NEW QUESTION: 48
□□□ "□□ □□ □□ □□"□ □□□□□□□ □□ □□□ □□□ □ □ □□□□?
A. □□ □ □□□ □□□ □□ □□ □□□ □□□□ □□ □□ □□
B. □□ □□ □□ □□□ □□ □□□□ □□ □□
C. FATF □□□ □□ □ □□ □□□ □□ □□ □□
D. □□ □□□ □□ □□ □□□ □□ □□□□ □□□□ □□□□□□□□.
Answer: B (LEAVE A REPLY)
Designating a country as being of "prime money laundering concern" allows the U.S. government to impose one or more of five special measures under Section 311 of the USA PATRIOT Act12. These special measures are intended to protect the U.S. financial system from the risks posed by the designated country, such as money laundering, terrorist financing, or other illicit activities. The fifth special measure, which is the most severe, authorizes the Treasury Department to prohibit U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for foreign financial institutions that involve the designated country12. Correspondent accounts are accounts that enable foreign banks to access the U.S. financial system and provide services to their customers, while payable-through accounts are accounts that allow foreign banks to offer their customers direct access to the U.S. financial system3. Closing these accounts effectively cuts off the designated country from the U.S. financial system and imposes significant costs and burdens on its financial sector.
Reference:
1: 311 Actions | U.S. Department of the Treasury
2: Press Releases - U.S. Department of the Treasury
3: Anti-Money Laundering Laws and Regulations USA 2023-2024

NEW QUESTION: 49
□□□□□□ □□ □□□□□ □ STR □□□ □□ □□□ □□ □□ □□□ □□□ □□□?
A. □□□ □□□ □ □□ □□□ □□ □□□ □□ □□□□ □□ □□
B. □□□□□□ □□□ □□ □□ □□□ □□ □ □□□ □□□ □□ STR □□ □□ □□□ □□□
C. STR□ □□□□ □□□ □□ □□□ □□ □ □□ □□□□ □□□
D. STR□ □□□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □.
Answer: (SHOW ANSWER)
An institution should focus on the appropriateness of having a centralized review of suspicious transactions and recommendations to file an STR to ensure consistency. This is because a centralized review process can help to avoid duplication, inconsistency, or omission of STRs, as well as to ensure compliance with regulatory requirements and internal policies. A centralized

review process can also facilitate the analysis of trends, patterns, and typologies of suspicious transactions across the institution, and enable the communication and coordination with relevant stakeholders, such as law enforcement, regulators, or other financial institutions.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 5, Section 5.3.1, page 1911 ACAMS CAMS Certification Video Training Course, Module 5, Lesson 5.3, video time 2:30-4:002 ACAMS CAMS Certification Practice Exam, Question 124, page 2843

NEW QUESTION: 50
□□□ □□ □□□ □□□□□ □□□ □□□ □□□□ □ □□□ □□□□□. □□□ □□□ □□ □□□ □□ □□□ □□ □□ □□□□□ □□ □□ □□□ □□□□.
□□ □□□ □□□ □ □□ □ □□ □□ □□□ □□□□□? (2□□ □□□□□.)
A. □□□□ □□□□□ □□□□□.
B. □□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □□ □□□□ □□□□□.
D. □□□ □□ □□□ □□ □□ □□
Answer: C,D (LEAVE A REPLY)
Wire transfers to high-risk jurisdictions and large cash deposits from a high-risk jurisdiction are two red flags that may indicate money laundering. These activities suggest that the customer is trying to move funds from or to a country that has weak anti-money laundering (AML) controls, or that is known to be a source or destination of illicit funds12. Wire transfers can also be used to obscure the origin or destination of the funds, or to layer transactions through multiple accounts or intermediaries3. Large cash deposits can indicate that the customer is trying to avoid the reporting or record-keeping requirements that apply to cash transactions, or that the customer is dealing with proceeds from illegal activities45. The other two options are not necessarily red flags, as the bank may have legitimate reasons to allow cash deposits, and the client may reside in a high-risk jurisdiction for legitimate reasons.

NEW QUESTION: 51
□□□ □□ □□ □□□ □□ □□ □□□□ □□□ □□ □□□□□ □□□ □□(PEP)□ □□□ □ □□ □□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ PEP□□ □□
B. □□ □□ □ □□
C. □□ □□ □ □ □□□□□ □□ □□
D. □□□ PEP □□ PEP□ □□□□ □□□□□ □□
Answer: (SHOW ANSWER)
According to the Basel Committee's paper on Customer Due Diligence for Banks1, banks should review their existing customer relationships on a regular basis, especially for higher risk categories of customers or business relationships. This includes identifying whether the customer or the beneficial owner is a PEP, either at the account opening stage or later, as a result of a change in the customer's circumstances or profile. The paper also states that banks should apply

a risk-based approach to determine the appropriate level and type of due diligence depending on the risk profile of the customer or the beneficial owner.

Reference:

Basel Committee on Banking Supervision, Customer due diligence for banks, October 20011

FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22), June 20132

ACAMS, CAMS Examination Study Guide, 6th Edition, Chapter 4

NEW QUESTION: 52

□□□ □□ □□ □□□ □□ □□ □□□ □□□□□. □□ □□□ □□□□□ □□ □□□ □□ □ □□□ □□ □□□□□?

A. □□□ □□ □□ □□□□ □□□□ □□ □□□ □□□ □□ □□ □□□□ □□□□□.

B. □□□ □ □□□□□□ □□□□ □□□□□□.

C. □□□ □□ □□ □□ □□ □3□□□ □□□□□ □□□□□.

D. □□□ □□ □□ □ □□□ □□ □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

The customer directing the payment of the money borrowed to an unrelated third party is a red flag for potential money laundering, as it could indicate layering or integration of illicit funds. The other options are not necessarily indicative of money laundering, although they could warrant further monitoring or due diligence depending on the customer profile and risk assessment.

Reference:

ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 3, page 97, section "Red Flags for Life Insurance Policies".

ACAMS CAMS Certification Video Training Course, Module 3, Lesson 3.2, "Red Flags for Life Insurance Policies".

NEW QUESTION: 53

□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□? (□ □□□ □□□□□.)

A. □□ □□ □□ □□ □□□ □□ □□□ □□□□.

B. □□ □□□□ □□ □□ □□□□ □□ □□□ □□ □□□ □□ □□□□ □□□ □□□□□.

C. □□□ □□□□ □□□ □□□ □□ □□□□ □□ □ □□ □□ □□ □□ □□□□ □□□□□.

D. □□□ □□□ □□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□.

E. □□ □□□□ □□ □□□ □□□□□ □□ □□□□□ □□□□□□.

Answer: (SHOW ANSWER)

A proper investigation of unusual transactions requires a mix of data analysis, contextual review, and expert judgment to assess potential risks.

Option B (Correct): Cross-referencing transactions with external factors (e.g., political events, commodity price fluctuations, news reports) helps identify potential links to illicit activities.

Option C (Correct): The relationship manager may provide insights into whether a transaction aligns with the customer's known profile and business activity.

Option D (Correct): A risk-based approach ensures that higher-risk transactions receive enhanced scrutiny, while lower-risk ones undergo standard monitoring.
Why Other Options Are Incorrect:
Option A (Incorrect): Focusing only on transaction amounts ignores contextual factors, such as unusual behavior in low-value transactions.
Option E (Incorrect): Automated alerts are valuable but cannot replace human analysis and judgment. Manual reviews remain necessary for complex cases.
Red Flags in Unusual Transactions:
Large or frequent transactions inconsistent with a customer's normal profile.
Payments from/to high-risk jurisdictions without a clear purpose.
Use of intermediaries or shell companies to move funds.
Best Practices for AML Investigations:
Use both qualitative and quantitative factors to assess transaction risks.
Collaborate with business units (e.g., relationship managers) to understand client behavior.
Apply a risk-based approach to allocate investigation resources efficiently.
Reference:
FATF Recommendation 10 (Customer Due Diligence)
Wolfsberg Group Guidance on AML Investigations
FinCEN Transaction Monitoring Guidelines

NEW QUESTION: 54
□□ □□□□□ □□ □□ □□□ □□□□□□ □□□ □ □□ □□ □□□ □ □□ □□ □□□ □□ □□□? (2□□ □□□□□.)
A. □ □□□ □□ □□□ □□ □□
B. □□□ □□ □□
C. □□□□□□□ □□ □□
D. □□ □□□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
The USA PATRIOT Act imposes several requirements on U.S. financial institutions when dealing with foreign financial institutions, especially those that pose a high risk of money laundering or terrorist financing. Two of these requirements are:
Performing enhanced due diligence on shell banks: A shell bank is a bank that has no physical presence in any country and is not affiliated with a regulated financial group. The USA PATRIOT Act prohibits U.S. financial institutions from opening or maintaining correspondent accounts for shell banks, and requires them to take reasonable steps to ensure that their correspondent accounts are not being used by shell banks indirectly12.
Performing due diligence on correspondent accounts: A correspondent account is an account established by a financial institution to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign financial institution. The USA PATRIOT Act requires U.S. financial institutions to collect and verify certain information about the foreign financial institution, such as its ownership, licensing, and anti-money laundering policies, and to

assess the risk of money laundering or terrorist financing associated with the correspondent account13.
Reference:
CAMS Certification Package - 6th Edition | ACAMS, Chapter 3: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), pages 82-84 CAMS Certifications: How to Get CAMS Certified | ACAMS, Candidate Handbook, page 14 ACAMS CAMS Certification Video Training Course - Exam-Labs, Video 3.4: Correspondent Banking and Money Laundering Risks

NEW QUESTION: 55
□□ □ □□ □□□ □ □□ □□□ □□□□□□□. 3□□ □□ □□ □□ □□□□ $9,500□ □□ □□□.
□□ □□□□ □□ □□ □□ □□□□ □□□□ □ □□ □□ □□□ □□□□□? (2□□ □□□ □□.)
A. □□□□□□ □□ □□□ □□□□.
B. □□ □□ □□□□ □□ □□□□
C. □□ □□□ □□□□ □□ □□□□□
D. □ □□□ □□□ □□ □□□ □□□□□.
Answer: B,D (LEAVE A REPLY)
These two options are potential red flags for money laundering or terrorist financing because they could indicate an attempt to avoid the reporting threshold of $10,000 for cash transactions, or to conceal the source or origin of the funds. According to the ACAMS Study Guide, some common indicators of money laundering are:
Transactions structured to avoid recordkeeping or reporting requirements Transactions inconsistent with the customer's profile or business activity Transactions involving the use of multiple accounts or locations Transactions involving high-risk jurisdictions or entities
Transactions involving cash or complex crypto assets The other two options are not necessarily red flags by themselves, as they could have legitimate explanations. For example, the restaurant could be located in a different city because of market demand, or the new account could demonstrate a steady flow of income because of the success of the business.
Reference:
ACAMS Study Guide for the CAMS Certification Examination - 6th Edition, Chapter 2, page 41-42
FFIEC BSA/AML Appendices - Appendix F - Money Laundering and Terrorist Financing Red Flags, page 1-2
4 Red Flags of Money Laundering or Terrorist Financing, page 1
Money Laundering Red Flags | Key Behaviours and Indicators, page 1

NEW QUESTION: 56
□□ □ □□□□□ AML □□ □□□ □□ □□□ □□□□ □□ □□□□□ □□□□ □□ □□ □ □□□□□?
A. □□ □□ □□ □□□□□ □□□ □□□□ □□□ □□□□.

B. □□□ □□□ □□□ □□□□□ □.
C. □□ □□□□ □□□ □□ □.
D. □□ □□□□ □□□□□ □□□ □ □□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
AML controls should be measured for effectiveness using quantifiable metrics.
Option D (Correct): The true positive/false positive ratio assesses the efficiency of AML detection.
Option A (Incorrect): The number of alerts alone does not measure effectiveness, as many could be false positives.
Option B (Incorrect): Client exits do not indicate whether an AML program is working properly.
Option C (Incorrect): High-risk customer onboarding must be monitored, but it does not indicate AML effectiveness.

NEW QUESTION: 57
□□□□ □□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□ □□□□ □□ □□ □ □□ □ □ □□ □□□ □□□□ □□□ □□□□ □□ □ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)
According to the Wolfsberg Principles on Correspondent Banking1, an institution should consider the following three elements in its enhanced due diligence process for higher risk respondent bank customers:
The quality of the respondent's AML and client identification controls: The correspondent should assess the adequacy and effectiveness of the respondent's AML policies, procedures, and systems, as well as its compliance with applicable AML laws and regulations. The correspondent should also verify that the respondent has implemented appropriate customer identification and verification measures, and that it maintains sufficient records of its customers and transactions.
A risk-based determination as to whether or not the respondent is a shell bank: The correspondent should ensure that the respondent is not a shell bank, which is defined as a bank that has no physical presence in any country and is not affiliated with a regulated financial group. The correspondent should also avoid establishing or maintaining relationships with banks that are known to allow their accounts to be used by shell banks.
Whether a Politically Exposed Person (PEP) has an interest or management role in the respondent: The correspondent should identify and assess the potential risks associated with any PEPs who have an ownership or management interest in the respondent, or who are customers of the respondent. The correspondent should apply enhanced scrutiny and monitoring to such relationships, and obtain senior management approval before establishing or continuing them.
Reference:
Wolfsberg Correspondent Banking Principles 2022 by the Wolfsberg Group, October 2022.

NEW QUESTION: 58

Financial Action Task Force□ □□ □□□ □□□ □□ □□ □□□ □□ □□□ □□ □□ □□ □ □□ □□□ □□□?

A. □□□ □□ □□ □□ □□□ □□□□□□□□.

B. □□ □□ □□□□□ □□□□□ □□ □□□ □□

C. □□□□□□ □□ □□□□□ □□□□□ □□ □□ □□□ □□□□□□.

D. □□□□□□ □□ □□□□□ □□ □□□ □□

Answer: C (LEAVE A REPLY)

According to the Financial Action Task Force (FATF), a country's financial intelligence unit (FIU) plays a key role in safeguarding against money laundering and terrorist financing. One of the main functions of an FIU is to receive, analyze, and disseminate suspicious activity reports (SARs) submitted by financial institutions and other obligated entities. By analyzing SARs, an FIU can identify trends, patterns, and other intelligence related to money laundering and terrorist financing, which can assist in the pursuit of criminal activity. While an FIU may also generate currency transaction reports (CTRs) or other types of financial reports, these functions are not specific to safeguarding against money laundering and terrorist financing. Similarly, while monitoring monthly public statistics on the economy may be an important aspect of macroeconomic analysis, it is not a specific role of an FIU in safeguarding against money laundering and terrorist financing.

NEW QUESTION: 59

□□ □□ □□ □□□ □□□ □□ □□□ □ □□ □□□ □□□□□□? 3□□ □□□ □□□□□□

A. □□□ □□□□ □□ □□ □□□□□ □□□□□ □□ □□

B. □□□□□□ □□□ □□□□□□□□ □□ □□□ □□□□ □□□□□□ □□□□ □□

C. □□□□ □□ □□□ □□ □□ □□

D. □□□ □□, □□ □□ □□□□ □□ □□□ □□□ □□ □□ □□ □□□

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

According to the Anti-Money Laundering Specialist (the 6th edition) resources, electronic funds transfers (EFTs) are transactions that involve the movement of funds electronically from one account to another, either within the same financial institution or across different institutions, domestically or internationally1. EFTs can be used for legitimate purposes, such as facilitating trade, commerce, and remittances, but they can also be exploited by money launderers to conceal the origin, ownership, and destination of illicit funds2. Some of the indicators of money laundering associated with using EFTs are:

Funds transfers to or from a financial secrecy haven without an apparent business reason. Financial secrecy havens are jurisdictions that offer a high degree of banking secrecy, low or no taxes, lax regulation and supervision, and weak or non-existent anti-money laundering and counter-terrorist financing (AML/CTF) measures3. Money launderers may use these havens to hide their illicit funds, evade taxes, and avoid scrutiny from authorities. Funds transfers to or from these havens without a clear or plausible explanation may indicate an attempt to launder money or finance terrorism.

Funds transfers are received or sent from the same person to or from different accounts. This may indicate a layering technique, which is the process of moving funds through multiple accounts, institutions, or jurisdictions to obscure the audit trail and the source and ownership of the funds4. Money launderers may use this technique to avoid detection, reporting, or freezing of their funds by authorities or financial institutions.
Payment or receipts with no apparent link to legitimate contracts, goods or services. This may indicate a trade-based money laundering technique, which is the process of using trade transactions to disguise the movement of illicit funds, either by over- or under-invoicing, misrepresenting the quantity or quality of goods, or falsifying documents. Money launderers may use this technique to transfer value across borders, evade taxes or customs duties, or justify the movement of funds that have no legitimate origin or purpose.
The other option is incorrect because:
Regular and frequent transfers from the account of a large company said to be payment for goods bought on credit is not necessarily an indicator of money laundering associated with using EFTs. This may be a normal business practice for some companies that have a high volume of transactions or a long-term relationship with their suppliers or customers. However, this may also be a red flag if the company is not well-known, has no physical presence, has no apparent business activity, or is located in a high-risk jurisdiction. Therefore, this option requires further investigation and verification before concluding that it is an indicator of money laundering.
Reference:
1: ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 104 2: ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 105 3: ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 107 4: ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 106 : ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 108

NEW QUESTION: 60
□□ □□□ □□ □□□□□□ □□ □□□ □□ □□ □□□ □□□□□□?
A. □□ □□□ □□□ □□□□□□ □□□ □□□ □□□ □□□□□.
B. □□ □□□ □□□□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□.
C. □ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□ □□□□□□□.
D. □□ □□□ □□ □□□□□ □□□ □□□ □□ □□□□□□□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
Money laundering through capital markets often involves pump-and-dump schemes, wash trading, and layering funds through rapid trading activity.
Option A (Correct): A sudden spike in demand for a low-priced security is a red flag for pump-and-dump schemes, where criminals manipulate the market to inflate stock prices artificially before selling off shares for a profit.
Option B (Incorrect): A gradual decline in trading volume and price does not indicate suspicious activity related to money laundering.
Option C (Incorrect): An increase in demand for ETFs is common and not necessarily linked to money laundering.

Option D (Incorrect): Holding securities in one specific emerging market may indicate a geographic investment strategy, not necessarily money laundering.
Common Money Laundering Typologies in Capital Markets:
Pump-and-Dump Schemes - Fraudulently inflating stock prices to cash out illicit funds.
Wash Trading - Conducting self-trades to create an illusion of high market activity.
Layering Funds Through Rapid Trading - Engaging in frequent buy-and-sell orders to obfuscate the origin of funds.
Best Practices for AML in Capital Markets:
Monitor unusual trading volume and price fluctuations.
Use AI-driven surveillance systems to detect manipulative behavior.
Investigate transactions involving offshore brokers or shell entities.
Reference:
FATF Report on Money Laundering in Capital Markets
SEC and FINRA Guidance on Market Manipulation Risks
Wolfsberg Group Principles for Capital Markets AML Compliance

NEW QUESTION: 61
□□□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□ □□□□□□. □□□ □□□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□ □ □□ 3□□ □□□ □□□□□ □□□□□□. □□ □□□ □□ □□□□ □□□ □□□ □□□□. □□□□□□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□□.
A. □□ □□□□ □□□ □□□□□□ □□□ □□□□□.
B. □□□ □□□□ □□□□□ □□ □□□ □□□□.
C. □□□□□□□(Transparency International) □□□ □□ □□□□ □□□□ □□ □□□□.
D. □□ □□□□ □□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)
This is the correct answer because the institution must ensure that the beneficiaries of the transfers are not on a terrorist watch list, such as the United Nations Security Council Consolidated List, the U.S. Treasury Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons List, or the European Union Terrorism List. These lists contain the names of individuals, entities, and groups that are subject to sanctions or other measures due to their involvement or association with terrorism or terrorist financing. The institution must screen the beneficiaries of the transfers against these lists and report any matches or hits to the relevant authorities. Failing to do so may expose the institution to legal, regulatory, or reputational risks, as well as facilitate the financing of terrorism.
Reference:
ACAMS CAMS Certification Video Training Course1, Module 3: International AML/CTF Standards, Lesson 3.2: International AML/CTF Standards ACAMS CAMS Study Guide, 6th Edition2, Chapter 3: International AML/CTF Standards, Section 3.2: International AML/CTF Standards, pp. 57-58 ACAMS CAMS Examination Preparation Seminar, 6th Edition3, Chapter 3: International AML/CTF Standards, Section 3.2: International AML/CTF Standards, Slide 12

NEW QUESTION: 62

AML □□ □□□□□ □□□□ □□□□□ □□□□ □□ □□ □□ □ □□ □□□□ □□ □□□□□□?

A. FIU□ □□□□□□ □□ □□□(SAR)□ □□□□ □□ □□□□□ □□ □□□□ □□□□ □ □□ □□ □ □□□□□□ □□□□.

B. □□□□□□ □□□□ □□□□ □ □□ □□□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□□.

C. □□□□ □□□□□ □□□□□ □□ □□□□□□ AML □□ □□□□□ □□ □□ □ □□ □□□□ □□ □□□.

D. □□□□ □□ □□□□□□□(FIU)□ SAR□ □□□□□ □□ □□□□ □□ □□□□ □□□□□□ □□ □□ □□□□.

Answer: (SHOW ANSWER)

AML compliance must balance data privacy laws with financial crime prevention.

Option A (Correct): FIUs must document the purpose of SAR-related data sharing under FATF Recommendation 29 and GDPR compliance standards.

Option B (Incorrect): Customers do not have the right to request redaction of personal data in SARs, as this would compromise AML enforcement.

Option C (Incorrect): Many jurisdictions permit information sharing for AML purposes under formal agreements (e.g., 314(b) USA PATRIOT Act, GDPR exemptions).

Option D (Incorrect): AML reporting requirements override opt-in privacy preferences due to the legal obligation to report suspicious activity.

NEW QUESTION: 63

□□ □□□□(USA PATRIOT Act)□ □□ □□ □□ □□(FIs)□ □□ □□ □□□□ □□ □□□□ □□ □ □□□□□ □□□□ □□□□□□?

A. □□ FIs□ □□ □□ □□□□ □□□□ □□ □□□□ □□□□ □ □□□□□.

B. US FIs□ □□ □□ □□□□ □□ □□ □□ □□□□ □□□□ □ □□□□ □□ □□□□□□ □□□□□.

C. □□ FIs□ □□ □□ □□□□ □□ □□□□ □□ □□□□ □□□□□ □□ □□□□ □□ □□ □□ □ □□□□□ □□□□□ □□□□.

D. □□ FIs□ □□ □□ □□□□ □□ □□ □□□□ □□□□□ □□ □□ □□ □□□□ □□(Financial Action Task Force)□ □□□□ □□□□ □□□□.

Answer: A (LEAVE A REPLY)

According to section 313 of the USA PATRIOT Act, a covered financial institution (generally any U.S. bank or broker dealer in securities) is prohibited from establishing, maintaining, administering, or managing a correspondent account in the U.S. for, or on behalf of, a foreign shell bank. A foreign shell bank is defined as a foreign bank that does not have a physical presence in any country. The only exception to this prohibition is if the foreign shell bank is a regulated affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the U.S. or a foreign country, respectively. In that case, the U.S. financial institution must obtain a written certification from the foreign bank that it does not provide banking services to any other foreign shell banks.
Reference:
Here's Why A Process Agent Is Required Under a Certification by a Foreign Bank, Cogency Global, September 2020.
Definition of "Foreign Shell Bank" and "Foreign Bank", FinCEN, April 2003.
USA PATRIOT Act, FinCEN, accessed February 2024.

NEW QUESTION: 64
□□ □ □□ □□□ AML □□□□□□ □□□□□□ □□ □□□ □□□□, □□□□ □□ □□ □□ □□ □□□ □□□□□□□□.
□□□ □□ □□□□□ □□□□□ □□ □□□ □□□ □□ □□?
A. □□□ □□□ AML □□ □□□□□ □□ □□□□□ □□□ AML □□ □□□ □□ □□□□□□ □□□ □□□ □□ □□ □□□ □□□ □□ □ □ □□□□.
B. □□ □□□ □□□ AML □□ □□□□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□□ □□ □□□□ □□□□.
C. □□□ □□□ AML □□ □□□□□ □□□ □□ □□□ □□□ AML □□ □□□ □□ □□□ □□□ □ □ □□ □□□ □□□□□□.
D. □□□ □□□ AML □□ □□□□□ □□ □□□□□ AML □□ □□□□□ □□ □□□ □□ □ □ □□ □□ □□□ □□ □□ □□□□.
Answer: (SHOW ANSWER)
Senior management and AML officers may face personal liability if they knowingly allow AML violations to persist.
Option A (Correct): If senior management or the AML officer was aware of violations and failed to act, they could face regulatory or criminal liability.
Option B (Incorrect): Criminal liability depends on intent and negligence-an AML officer is not automatically prosecuted because a bank receives a regulatory order.
Option C (Incorrect): Liability extends beyond the AML officer-other senior executives can also be held accountable.
Option D (Incorrect): Violations can result in both civil and criminal prosecution, depending on the severity.
Legal Risks for AML Compliance Failures:
Civil penalties (fines and sanctions) for AML program deficiencies.
Criminal charges if executives knowingly ignore violations.

Regulatory enforcement actions leading to license revocation.
Reference:
USA PATRIOT Act Section 352 (AML Compliance Program Requirements)
FinCEN Guidelines on AML Compliance Officer Liability
FATF Recommendation 35 (Sanctions for AML Non-Compliance)

NEW QUESTION: 65
□□ □□□□□ □□□ □□ □□□ □□□□□ □□□?
A. □□□ □□□ □□ □□ □□□ □ □□□ □□□.
B. □□ □□□ □□□ □□□ □□□□□□ □□□□□ □□□□□□□.
C. □□ □□□□□ □□□ □□ □□□ □□□□□□.
D. □□□ □□ □□□ □□□ 5□ □ □□□ □□□ □□ □□□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
Company ownership is held in bearer share form. Bearer share ownership can make it difficult to identify the actual owners of a company and is therefore considered a high risk for money laundering or terrorist financing. Enhanced due diligence measures may include obtaining additional identification and ownership information, conducting more frequent reviews of the account, and monitoring transactions more closely.

NEW QUESTION: 66
□□ □□ □□ □□□ □□ □□□□□□ □□□ □ □□ □□□ □□□ □ □□ □□ □□ □□□□□ □□ □□ □□□ □□□ □□□□□ □□ □□ □□□ □□ □□□□□□ □□□□□□□. □□ □ □□ □ "□□□ □□" □□□ □□□□□ □□ □□□□□□ □□ □□□ □□□□□?
1.□□□□□□ □□, □□□ □□ □ □□ □□□□□.
2. □□□ □□ □ □□□□□□ □□.
3. □□□ □□ □□.
4. □□□□□ □□, □□ □□ □□□ □□□ □□.
A. 1, 2, 3□
B. 1, 2, 4□
C. 1, 3, 4□
D. 2, 3, 4□
Answer: C (LEAVE A REPLY)
These are the information that can help the correspondent bank to assess the risk profile, the regulatory compliance, and the operational capacity of the respondent bank, and to verify its identity and legitimacy. The correspondent bank should obtain and verify the following information about the respondent bank:
Respondent's management, nature of license, and major business activity. This can help the correspondent bank to understand the governance, the legal status, and the core functions of the respondent bank, and to evaluate its reputation, integrity, and competence.
The quality of supervision in the home country. This can help the correspondent bank to determine the level of oversight and regulation that the respondent bank is subject to, and to

identify any potential gaps or weaknesses in the anti-money laundering and counter-terrorist financing (AML/CTF) framework of the home country.
Respondent's location, in particular the existence of a real physical presence. This can help the correspondent bank to verify the actual existence and operation of the respondent bank, and to avoid dealing with shell banks or banks located in high-risk or non-cooperative jurisdictions.
The other option is not necessarily information that should be included to establish a rigorous "Know Your Respondent" procedure, although it may have some relevance or importance depending on the circumstances and the nature of the correspondent relationship. Option 2 describes computer equipment and software capability, which may be useful to assess the technical and operational compatibility and efficiency of the respondent bank, but it is not essential to evaluate its risk or compliance level.
Reference:
ACAMS CAMS Certification Video Training Course - 6th Edition1
Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)2 ACAMS CAMS Study Guide - 6th Edition, Chapter 7, pages 154-155
: https://www.acams.org/wp-content/uploads/2019/09/ACAMS-CAMS-Study-Guide-6th-Edition-Chapter-7.pdf

NEW QUESTION: 67
□□ □ □□□ □□□ □□□□ □ □□ □□□□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□□□□ □□ □□□ □ □□ □□□.
B. □□ □□□□□ □□□□ □□□□.
C. □□□ □□ □□□ □□□□ □□.
D. □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□□□.
Answer: C (LEAVE A REPLY)
Internet gambling is an ideal web-based money laundering method because it allows criminals to move funds across borders quickly, anonymously, and with minimal oversight12. Internet gambling sites can facilitate the placement, layering, and integration stages of money laundering by accepting cash deposits, issuing virtual credits, allowing bets on various games, and paying out winnings through different payment methods12. Internet gambling also poses challenges for law enforcement and regulators, as it operates in a complex and dynamic environment that involves multiple jurisdictions, service providers, and technologies12.
Reference:
ACAMS CAMS Study Guide (the 6th edition), Chapter 2: Money Laundering Risks and Methods, page 671 ACAMS Today, The Growing Threat of Online Gambling Money Laundering2

NEW QUESTION: 68
□□□□□□□ □□□□□□ □□□ □ □□ □□ □□□ □□□□□?
A. □□□□□ □□□ □□□ □□
B. □□□ □□□ □□□□
C. □□□□□□ □□□□ □□□ □□□ □□□□ □□

D. □□□ □□ □ □□□□ □□□□□ □□□ □□
Answer: A (LEAVE A REPLY)
According to the ACAMS CAMS Study Guide, one of the most common methods of placement is to deposit cash into a bank account, either directly or through intermediaries. This allows the money launderer to introduce the illicit funds into the legitimate financial system, and to create a paper trail that can be used to justify the source of the funds. However, this method also exposes the money launderer to the risk of detection by the bank's anti-money laundering (AML) policies and procedures, such as customer identification, transaction monitoring, and reporting of suspicious activities1.
Reference:
ACAMS CAMS Study Guide, 6th Edition, page 271

NEW QUESTION: 69
□ □□ □□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□ □□ 20□□ □□□□ □□□□ □□□□. □□□ □□□ □□□ AML □□□□ □□ □□□ □□□ □□□? (2□□ □□□□□.)
A. □□□ □□□□ □□□□ □□ □□□ □□ □ □□ □□ □□□ □□□□□□□.
B. □□□ □□ □□□ □□□□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□.
C. N □□□ □□ □□ □□□□□ □□□□ □□ □□□ □□ □□□ □□□□□.
D. □□□ □□□□ □□ □□□ □ □□ □□□ □□□□□.
E. □□ □□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □ □□ □□□ □□□□□.
Answer: A,B (LEAVE A REPLY)
According to the ACAMS CAMS Study Guide, 6th Edition, Chapter 4, Section 4.2, the AML Specialist at a bank should take the following actions upon receiving a confidential alert from law enforcement about suspected money launderers:
Involve the bank's legal and compliance function to address the gravity of the matter and ensure that the bank's response is appropriate and lawful. The legal and compliance function can also advise on the bank's obligations and rights under the relevant laws and regulations, such as the General Data Protection Regulation (GDPR), the Bank Secrecy Act (BSA), and the USA PATRIOT Act.
Perform a search on the bank's client data platform to determine if the bank has had any business with the named individuals or any related parties. The search should include current and past accounts, transactions, wire transfers, and other relevant records. The AML Specialist should also review any existing customer due diligence (CDD) and enhanced due diligence (EDD) information on the potential suspects and update them as necessary.
The other options are not recommended or required actions for the AML Specialist at a bank in this scenario:
Sending out an email to all of the bank's client advisors to request information on any of the individuals could compromise the confidentiality of the alert and expose the bank to legal and

reputational risks. It could also alert the suspects or their associates and hinder the law enforcement investigation.
Reporting findings back to law enforcement only if they are of any significance is not sufficient or compliant with the bank's obligations to cooperate with law enforcement and report any suspicious activity. The AML Specialist should report any relevant information or findings to law enforcement as soon as possible, regardless of their significance, and follow the established procedures and protocols for information sharing and reporting.
Responding to law enforcement that their request without a judicial order would breach the bank's GDPR duty with respect to its clients is not accurate or helpful. The GDPR does not prohibit the bank from sharing personal data with law enforcement for the purposes of preventing, detecting, or investigating money laundering or other criminal activities, as long as the bank has a legal basis and safeguards for doing so. The bank should consult with its legal and compliance function to determine the best way to respond to the law enforcement request and balance its GDPR obligations with its anti-money laundering (AML) duties.
Reference:
ACAMS CAMS Study Guide, 6th Edition, Chapter 4, Section 4.2
General Data Protection Regulation (GDPR)
Bank Secrecy Act (BSA)
USA PATRIOT Act

NEW QUESTION: 70
□□ □□□□□ □□□□ □□ □□□ □□(US) □□□ □□ □□□ □□□□□□ □□□. □ □□ □□□ □□ □□□□ □□ □□□ □□ □□□□ □□□ □□□□□.
USA PATRIOT Act□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□?
A. □□□□ □□□□□ □□□□□ □□□ □□□□ □□
B. □□□□□ □□□ □□□□□ □□□□□ □□
C. □□□□□ □□□□ □□ □□□ □□□ □□ □ □□ □□ □ □□
D. □□□□ □□□ □□□□ □□□ □□□□ □ □□□□□□ □□ □□ □□
Answer: (SHOW ANSWER)
through account transactions
Explanation:
Under the USA PATRIOT Act, a U.S. bank that maintains a correspondent account for a foreign bank operating under an offshore license must obtain from the foreign bank the name and address of a person residing in the United States who is authorized to accept service of legal process for records related to the correspondent account1. This requirement is intended to facilitate the U.S. authorities' access to information and records regarding the correspondent account and its underlying transactions, especially in cases where the foreign bank is located in a jurisdiction that does not cooperate with U.S. law enforcement or regulatory requests2.
Reference:
USA PATRIOT Act, Section 319(b)(2)(A)1

ACAMS, CAMS Examination Study Guide, 6th Edition, Chapter 5, pp. 151-152 Wolfsberg %27s_CBDDQ_Capacity_Building_Guidance_Final%20V1.1.pdf

NEW QUESTION: 71

□□ □□ □□□ SAR(□□□□□□ □□ □□□) □□ □□□ □□ Financial Action Task Force □ □□ □□□□□ □□□ □□□ □□□□□□?

A. □□ □□□ AML □□□□□ □□□□□ □□□□ □□□□□ □□□□□ □□□ □□ □□□ □□□□□ □□□.

B. □□ □□□ SAR □□ □ □□ □□□ □□□□□□ □□ □□□ □□□ □□□ □□□.

C. □□ □□□ SAR □□□ □□ □□□ SAR □□□□□□□ 5□ □□ □□□□□ □□□.

D. □□ □□□ □□ □□□ □□□ □□□□□ □□□ □□ □□□ □ □□□□□.

Answer: A (LEAVE A REPLY)

According to the Financial Action Task Force (FATF) standards for suspicious activity reports (SARs) information sharing within a financial group, "Financial institutions should establish adequate procedures to ensure that confidentiality of information is maintained and that information is only used for purposes permitted under national law. Where the parent institution is located in a country that does not permit such sharing, financial institutions should take measures to address this limitation" (CAMS Manual, 6th Edition, page 476). Therefore, financial institutions must establish sufficient safeguards concerning the confidentiality of information shared for AML purposes.

NEW QUESTION: 72

□□ □□(EU) □□□ □□ □□□ □□ □□ □□□ □□ □□□□. USA PATRIOT Act Section 311□ □□ □□ □□□ EU □□□□□ □□□□(payable-through) □□□ □□□ □□□ □□□ □ □ □□ □□□ □□□□□□. □□ □ □□□ □□□ □□ EU □□□ □□□□□ □□□□□ □□ □□ □ □□□ □ □□□ □□□□□?

A. □□□ □□□ □□ □□□ □□ □□□ □□□□□ □□□ □□□.

B. □ □□□ □□□ □ □□ □□□ □□ □□ □□□ □□□□□.

C. EU □□□ □□□ □□□ □□□□□ □□□□□□ □□□□□□.

D. EU □□□ □□ □□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

Under USA PATRIOT Act Section 311, the U.S. government can impose special measures against a foreign jurisdiction, institution, or transaction that is of primary money laundering concern1. These measures can range from requiring additional recordkeeping and reporting to prohibiting or restricting the opening or maintaining of correspondent or payable-through accounts for the designated entity2. A payable-through account is a type of correspondent account that allows customers of a foreign bank to access the U.S. financial system by writing checks or making wire transfers from the foreign bank's account at a U.S. bank3.

In this case, the U.S. government has enacted special measures against a designated entity that has a payable-through account with an EU bank, which in turn has a correspondent banking relationship with a U.S. bank. One of the possible actions that the U.S. bank might be required to

take regarding the EU bank's services for the designated entity is to obtain additional information about customers permitted to use this account. This is to ensure that the U.S. bank can identify and monitor the transactions and activities of the designated entity and its customers, and to prevent any money laundering or terrorist financing risks4.
The other actions listed are not likely to be required by the U.S. government under Section 311. Ensuring the designated entity's confidential information is not shared with other entities is not a special measure, but a general obligation of any financial institution under privacy laws. Verifying that the EU bank serves the designated entity is not a relevant action, since the U.S. government has already designated the entity as a primary money laundering concern. Performing enhanced due diligence on the EU bank is not a specific action related to the payable-through account, but a broader requirement for any correspondent account under Section 312 of the USA PATRIOT Act5.
Reference:
1: USA PATRIOT Act | FinCEN.gov1 2: 311 Actions | U.S. Department of the Treasury2 3: Overview of Correspondent Banking and "De Risking" Issues - CRS Reports3 4: U.S. TREASURY DEPARTMENT OFFICE OF PUBLIC AFFAIRS4 5: Fact Sheet: Overview of Section 311 of the USA PATRIOT Act5

NEW QUESTION: 73
□□□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□□ □□ □□□ □□□□. □□□ □□□ □□□□ □□ □□□ □□ □□ □□□□ □□ □□ □□ □□ □□ □□ □□ □ □□□□ □□□□□ □□□ □□□□□□ □□□ □□□□□. □□□□ □□□□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□□ □□□□□.
□□□□ □ □□□ □□□ □□□□ □□□?
A. □□□ □□ □□□□ □□
B. □□ □□□ □□□ □□ □□ □□□ □□□□□.
C. □□□□□ □□ □□ □□□□□□ □ □□ □□□□□ □□□□□ □□□□□.
D. □□□ □□□ □□□ □□ □□□□ □□□ □□ □□□□ □□ □□ □□□□□.
Answer: B ([LEAVE A REPLY])
The branch manager should conduct further investigation before taking any other action, as this activity may indicate possible money laundering or fraud. The branch manager should review the transaction records of the customers and the teller, and look for any unusual or suspicious patterns, such as large or frequent cash deposits, round amounts, structured transactions, or inconsistent information. The branch manager should also interview the teller and the customers, and ask them about the nature and purpose of their relationship, the source and use of funds, and the reason for choosing the same teller. The branch manager should document the findings and report any suspicious activity to the appropriate authorities, if necessary.
Reference:
CAMS Study Guide, 6th Edition, Chapter 3, Section 3.21
CAMS Study Guide, 6th Edition, Chapter 4, Section 4.21
CAMS Exam Questions and Free Practice Test, Question 322

NEW QUESTION: 74

□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□ □□□□□□ □□□□□□ □□ □□□ □□ □ □□□□ □□□.

A. □□ □□ □□□□□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□□□□ □□□ □□ □□ □ □□□□.

B. □□ □□□ □□□□□ □□□ □□□ □□□□□□□ □□□ □□ □□□ □□ □□ □□□□□ □ □ □□ □□□ □□□□.

C. □□ □□□ □□□□□ □□□□□ □□□ □□, □□ □□ □□ □ □□□□□□ □□□□□.

D. □□□ □□□□□ □□ □ □□□□□□□ □□□ □□, □□□□□, □□ □ □□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

Customer due diligence (CDD) is a key component of anti-money laundering (AML) and counter-terrorism financing (CTF) compliance. CDD helps financial institutions identify and verify their customers, assess their risk levels, and monitor their transactions for suspicious activity.

One of the main objectives of CDD is to understand the nature and purpose of customer relationships, which involves collecting and analyzing relevant information about the customer's business activities, expected transaction patterns, source and destination of funds, and beneficial ownership. This information helps financial institutions develop a customer risk profile, which is a tool to measure and manage the risk exposure of each customer.

A customer risk profile reflects the financial institution's risk appetite, which is the level and type of risk that the institution is willing and able to accept. By comparing the customer's risk profile with the institution's risk appetite, the institution can determine if the customer operates in line with the firm's expectations and requirements for a specific industry segment. For example, if the institution has a low risk appetite for customers involved in high-risk sectors such as gambling, cryptocurrency, or arms trade, it can use the customer risk profile to identify and mitigate any potential risks associated with such customers.

Therefore, to understand if the customer operates in line with the firm's risk appetite for a specific industry segment, a financial institution must obtain sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile.

Reference:

A Guide to Customer Due Diligence for Financial Institutions

Customer Due Diligence Guide: Main Requirements, Best Practices & Checklist Financial Crimes Enforcement Network Issues New Frequently Asked Questions on Customer Due Diligence Requirements ACAMS CAMS Certification Study Guide 6th Edition

NEW QUESTION: 75

□□□□□□□ □□□□□ □□□□□□□ □□□□□□ □□□□□ □□□□□ □□□□.

□□□□□□ □□□□□ □□□□□ □□ □□□□□ □□□□□ □□□□□□?

A. □□ □□

B. □□ □□□

C. □□□□□□□ □□□□
D. □□□ □□ □□ □□□/□□□
Answer: D (LEAVE A REPLY)
A qualified independent party/auditor is the most effective resource to evaluate the effectiveness of an anti-money laundering program. This is because an independent auditor can provide an objective and unbiased assessment of the program, identify any weaknesses or gaps, and make recommendations for improvement. An independent auditor can also verify the compliance of the program with the relevant regulations and best practices, and test the adequacy and functionality of the internal controls, customer due diligence processes, and transaction monitoring systems. An independent auditor can also help an organization prepare for regulatory examinations and audits, and avoid potential penalties or sanctions.
Reference:
The document titled "Frequently Asked Questions Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs" published by the Financial Crimes Enforcement Network (FinCEN) in July 2010. You can access it by clicking here.
The document titled "AML Audit: How to Effectively Assess Your Compliance Program" published by Alessa in May 2023. You can access it by clicking here.
The document titled "Mutual Evaluations" published by the Financial Action Task Force (FATF). You can access it by clicking here.

NEW QUESTION: 76
□□ □ □□ □□□ AML □□□□□□ □□□□□□ □□ □□□ □□□□, □□□□ □□ □□ □□ □□ □□□ □□□□□□□□.
□□□ □□ □□□□□ □□□□□ □□ □□□ □□□ □□ □□?
A. □□□ □□□ AML □□ □□□□□ □□ □□□□□ □□□ AML □□ □□□ □□ □□□□□□ □ □□ □□□ □□ □□ □□□ □□□ □□ □ □ □□□□.
B. □□ □□□ □□□ AML □□ □□□□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□□ □ □ □□□□□ □□□□.
C. □□□ □□□ AML □□ □□□□□ □□□ □□ □□□ □□□ AML □□ □□□ □□ □□□ □□□ □ □ □□ □□□ □□□□□.
D. □□□ □□□ AML □□ □□□□□ □□ □□□□□ AML □□ □□□□□ □□ □□□ □□ □ □ □□ □□ □□□ □□ □□ □□□□.
Answer: A (LEAVE A REPLY)
Under U.S. AML laws, senior management and AML officers can face personal liability for compliance failures.
Option A (Correct): If senior management was aware of violations but failed to act, they can be held personally liable under FinCEN regulations and the Bank Secrecy Act (BSA).
Option B (Incorrect): Criminal prosecution depends on willful misconduct and does not apply automatically when a bank receives a regulatory order.
Option C (Incorrect): Other senior executives (e.g., CEOs, compliance officers) can also be held liable, not just the AML officer.

Option D (Incorrect): Criminal liability is possible for willful AML violations, not just civil penalties.

NEW QUESTION: 77

□□ □□ □□□□□ □□ □□□ □□□□□□ □□□□□ □□□□□ □□ □□ □□□ □□□□□ □□ □? (2□□ □□□□□□.)

A. FinCEN□ □□□ □□ □□ □□□(SAR)□ □□□□□□ □□□□□ □□□□□ □ □□□ □□□ □□□□□□.

B. □□□□□□ □□ □□ □□□□□ □□□ □□□ □□□□□ □□□□□□□ □□ □□□□□ □□□, □□□□□□ □□□□□□.

C. □□□ □□ □□ □ □□□□ □□ □□□□ □□□ □□ □□□□ □□□□□□ □□ □□□□□ □□□ □□ □□□□□□.

D. □□□ AML □□□ □□□□□□ □□ □□□□□ □□□□□□ □□□□□ □□□□□□ □□□□□□.

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: 78

AML □□□ □□□ □ □□□□ □□ □□□ □□□□ □ □□ □□□ □□□□□?
(3□□ □□□□□□.)

A. □□□□□ □□□ □□ □□, □□□□□ □□ □□□ □□□□□□ □□□ □□□□□□.
B. □□□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□ □□□□□□.
C. □□ □□ □□ □□□ □□□□□□ □□ □□□□□ □□□□□□.
D. □□ □□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□□ □□□□□□.
E. □□□ □□□ □□□□□ □□□ □□□ □□□□□□.
F. □□ □ □□ □□□ □□□□□ □□ □□□ □□□□□□□.

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

When investigating an AML event, the following techniques would be used to investigate suspected mule accounts:

A . Determine if the suspected accounts are being accessed by a common person, telephone number, or device. This can help identify if the accounts are controlled by the same person or group, or if they are part of a larger network of mules. It can also help detect if the accounts are opened using synthetic identities or stolen credentials12.

B . Reconcile the stated purpose of the account with actual transaction history and compare with peer groups. This can help assess if the account activity is consistent with the customer profile, risk rating, and expected behavior. It can also help identify anomalies, such as sudden changes in transaction patterns, large or frequent transfers, or transactions with high-risk jurisdictions or entities12.

E . Establish the frequency with which the funds are moved in and out of the accounts. This can help measure the velocity and volume of the funds flowing through the accounts, which can indicate if the accounts are used for layering or integration of illicit funds. It can also help detect if the accounts are used for smurfing, which is a technique of breaking down large amounts of cash into smaller deposits to avoid detection or reporting thresholds13.

Reference:
CAMS Study Guide (the 6th edition), page 1841
Mule accounts: how to track them down - Linkurious2
Money Mules - FBI3

NEW QUESTION: 79

□□ □□□ □□□□□ □□□ □□ □□□ □□□ □□□□□ □□, □□□□□□ □□□ □□□ □□ □ □□ □□□□□.

A. Egmont □□□ □□ □□□ □□□□□□.
B. □□ □□ □□□ □□ □□ □□□ □□□□□□.
C. □□ □□ □□□□□□(Financial Action Task Force), □□□□□□□□(OECD) □□ □□ □□ □□□ □□□□□ □□□ □□□□□.
D. □□ □□□ □□ □□ □□□□□ □□ □□□□□.

Answer: A (LEAVE A REPLY)

The Egmont Group of Financial Intelligence Units (FIUs) is a global network of FIUs that facilitates and promotes the exchange of information, knowledge, and cooperation among its members to combat money laundering, terrorist financing, and other financial crimes1. The Egmont Group has developed operational guidance for international cooperation and information exchange among FIUs, which includes channels, procedures, and forms for making and receiving requests2. Filing a request under Egmont guidelines is therefore a common and effective way for a regulatory body to obtain international assistance in a money laundering inquiry, as it ensures that the request is made through the appropriate and secure channel, and that it meets the standards and expectations of the requested FIU.
Reference:
1: Home - Egmont Group
2: EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS OPERATIONAL GUIDANCE FOR ...

NEW QUESTION: 80
□□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□□□?
A. □□□□
B. □□ □□
C. □□□□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
International wire transfers are considered to be of highest money laundering risk because they can facilitate the rapid and anonymous movement of funds across borders and jurisdictions, making it difficult for law enforcement and regulators to trace the origin and destination of the funds, and to identify the beneficial owners and controllers of the accounts involved. International wire transfers can also be used to layer and integrate illicit proceeds into the legitimate financial system, by disguising the source, ownership, and purpose of the funds. International wire transfers can involve multiple intermediaries, complex payment chains, and inconsistent or incomplete information, which can increase the risk of money laundering and terrorist financing. Therefore, international wire transfers are subject to enhanced due diligence, record-keeping, and reporting requirements under various anti-money laundering and counter-terrorist financing (AML/CTF) regulations and standards, such as the Financial Action Task Force (FATF) Recommendations1, the European Union (EU) Funds Transfer Regulation2, and the United States (US) Bank Secrecy Act3.
Reference:
1: FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, Recommendation 16 and Interpretive Note to Recommendation 16. 2: Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 5.6.2015, p. 1) 4 3: 31 U.S.C. §§ 5311-5330 and 31 C.F.R. Chapter X V

You cannot make international money transfers unless the money is credited to the account. So first priority saving account, subsequent risk international wire transfer
"A savings account, as well as a checking account, can be one of the riskiest financial instruments for money laundering operations given the ease with which it can be opened and operated".

NEW QUESTION: 81
□□□□□ □□□□ □□ □□□□□□□□□□ □□□□□□ □□□□ □□□. □ □□□ □□
□□ □□ □ □□ □□ □□ □□□□□?
A. □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□ □ □□□□.
B. □□□□□ □□ □□ □□□□□□ □□□□□.
C. □□□□□□□□□□ □□□ □□□ □□□ □□□.
D. □□□□ □□ □□□□ □□□□ □□□□□□ □□□□□ □□□.
Answer: (SHOW ANSWER)
The anti-money laundering officer (AML officer) is responsible for overseeing the implementation and effectiveness of the anti-money laundering (AML) program of a financial institution. The AML officer should have sufficient authority, independence, and access to resources to perform this role. Reporting to the Sales Director may compromise the independence and objectivity of the AML officer, as the Sales Director may have conflicting interests or incentives that could influence the AML officer's decisions or actions. The AML officer should report to a senior management level that is independent of business functions and has direct access to the board of directors or a relevant committee. This would ensure that the AML officer can communicate any AML issues or concerns to the board without any interference or undue influence from the business functions.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, Chapter 2, Section 2.2.1, page 41: "The AML officer should report to a senior management level that is independent of the business line and has direct access to the board of directors or a relevant committee." Money Laundering Reporting Officer: The Role Of MLRO, Section "Role Of Money Laundering Reporting Officer": "The MLRO should have independent monitoring and should be able to connect directly with people who make business decisions, such as senior management or the board of directors." Money Laundering Reporting Officer (MLRO)? | Dow Jones, Section "What is a Money Laundering Reporting Officer (MLRO)?": "A Money Laundering Reporting Officer (MLRO) is tasked with overseeing a firm's compliance with the Financial Conduct Authority's (FCA) rules on money laundering. ... The MLRO should have sufficient authority and independence within the firm to carry out their responsibilities effectively."

NEW QUESTION: 82
□□ □□□ □□□/□□□ □□□ □□□□□? (2□□ □□□□□.)
A. □□ □□
B. □□□□ □□
C. □□ □ □□□□ □□

D. □□ □□
E. □□ □□□□□□ □□
Answer: (SHOW ANSWER)
Money laundering has severe social and economic impacts, including increased crime rates, corruption and erosion of public trust. Money laundering fuels criminal activities by providing the necessary financial resources for criminals to continue their operations. As illicit funds circulate within the financial system, they enable the growth of criminal organizations and contribute to an increase in crime rates, including organized crime1. Money laundering also facilitates corruption and undermines public trust in financial institutions and the wider economy. This erosion of public trust is exacerbated by trade-based money laundering, which involves the manipulation of international trade transactions to disguise the origins of illicit funds2. Money laundering also weakens financial institutions by exposing them to reputational, operational, legal and regulatory risks. Money launderers exploit the vulnerabilities of financial systems and compromise their integrity and stability. Money laundering can also distort the allocation of resources, create inflationary pressures, and undermine the effectiveness of monetary policy3.
Reference:
1: Consequences Of Money Laundering Are: Understanding The Social, Economic, and Penalties Impacts1
2: Consequences of Money Laundering and Financial Crime2
3: Money laundering, its impact and consequences3

NEW QUESTION: 83
□□ □□(FI)□ AML □□ □□□ □□□□□ □□□ □□□□□□.
A. AML □□ □□□ □ □ □□ □□□□□□□□ □□□□□ □□ □□□□ □□ □□□□□□.
B. □□ AML □□ □□ □ □□□ □□□ □□□ □□□□□ □□ □□ □□.
C. □□□□□ □□□ □□ □□□□□ □□.
D. □□□ □□, □□□, □□ □ □□□ □□□ □□□ □□□ □□.
Answer: D (LEAVE A REPLY)
AML risk assessments are a key component of the risk-based approach to AML compliance, as required by the MLR 20171 and the FATF Recommendations2. AML risk assessments help FIs to identify, assess, and mitigate the money laundering and terrorist financing risks they face, taking into account their specific products, services, customers, and geographic locations. AML risk assessments also help FIs to allocate their resources and implement their AML policies and procedures in a proportionate and effective manner. AML risk assessments are not meant to be a one-off exercise, but rather an ongoing process that should be updated regularly to reflect changes in the FI's risk profile and the external environment.
Reference:
1: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
2: The FATF Recommendations - International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation

NEW QUESTION: 84
□□□ □□ □□□□ 10□ □□ □□□□ □□ □□□ □□□□ □□□□. □□□ □□□□ □□ □ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□ □□□□. □□ □□□□ □□□ □□ □ □ □□□□□ □□□□ □□□ □□ □□□ □□□□□. □□ □□ □□ □ □□ □□□ □□ □□ □□□?

A. □□□ □□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□□□ □□□ □□□□.

B. □□□ □ □□ □□□ □□□□□ □□□ □ □□ □□□ □□□□□ □□□ □□□□.

C. □□□ □□□ □□□ □□□□ □□□ □□□□□ □□□□.

D. □ □□□□□ □□□ □□ □□□ □□□ □□□ □□□□.

Answer: A (LEAVE A REPLY)

The most important risk factor in this scenario is the proposed offshore jurisdiction that is known for its strong privacy laws limiting access to customer information by law enforcement. This indicates that the customer may be trying to evade tax, hide the source or destination of funds, or engage in other illicit activities that could expose the bank to money laundering or terrorist financing risks. Offshore jurisdictions are often used by criminals to create complex corporate structures that obscure the beneficial ownership and control of the entities involved. The bank should conduct enhanced due diligence on the customer, the offshore company, and the nature and purpose of the transactions.

Reference:

ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 2, page 35-36, 38-39 ACAMS CAMS Certification Video Training Course, Module 2, Lesson 2.3, Offshore Financial Centers

1, CAMS Certification Package - 6th Edition | ACAMS, Offshore Financial Centers and Money Laundering

2, CAMS Certifications: How to Get CAMS Certified | ACAMS, CAMS Exam Outline, Domain 2, Task 2.3

NEW QUESTION: 85
□□ □□□□ □□ □□ □□□□□ □□□, □ □□□□ □□ □□□ □□□□ □□ □□□ □ □ □□□ □□□□ □□□□□.

□□ □□ □□□□ □□□ □□ □□□?

□□ □□ □□□□ □□□ □□ □□□?

A. □□□□□□□□

B. □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□ □□

C. □□□ □□□□ □□ □□ □□□□□ □□□□□.

D. □□ □□□□□ □□□ □□ □□□ □□□ □□□□□ □□□□□.

Answer: C (LEAVE A REPLY)

According to the ACAMS study guide, one of the best practices for dealing with law enforcement inquiries is to verify the identity and authority of the law enforcement officer before providing any information (p. 224). This is to ensure that the inquiry is legitimate and not a phishing attempt or a breach of confidentiality. The compliance officer should also document the inquiry and the information provided, and consult with legal counsel if necessary. The other options are not appropriate, as they may either violate the law, compromise the investigation, or create unnecessary work.

Reference:

ACAMS. (2020). Study Guide for the Certification Examination for Anti-Money Laundering Specialists (6th ed.). Miami, FL: ACAMS.

What Is An AML Officer1

NEW QUESTION: 86

□□□ □□ □□□ □□□□ □□□ □□□□□.

A. □□□□□ □□□ □□□ □ □□□ □□□.

B. □□ □□□ □□□ □□ □□□□□.

C. □□□ □□□□ □□□ □□□ □ □ □□□□.

D. Baring □□□ □ □□□ □□□ □□□ □ □□□ □ □□ □□□□.

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

According to the Anti-Money Laundering Specialist (the 6th edition) resources, one of the challenges of online financial technologies is the difficulty of verifying the identity and legitimacy of the customers and counterparties. This creates opportunities for money launderers and other criminals to exploit the anonymity and speed of online transactions to move and conceal illicit funds. The other options are not directly related to the money laundering risk posed by online financial technologies.

Reference:

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 5: Risk-Based Approach, page 133.

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 7: Money Laundering Risks and Methods, page 203.

NEW QUESTION: 87

□□ □□ □□□ □□ □□□ □□ □□□□□?

A. □□

B. □□□

C. □□

D. □□ □□

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

According to the ACAMS study guide, one of the insurance products that is particularly vulnerable to money laundering is annuity, which is "a contract that provides a series of payments over a specified period of time, usually for the life of the annuitant" (p. 223). Annuities can be used by money launderers to deposit large sums of illicit funds in a single transaction, or to receive regular payments from a legitimate source after paying the premiums with dirty money. Annuities can also be surrendered or transferred to third parties, making it difficult to trace the origin and destination of funds.

Reference:

ACAMS. (2020). Study Guide for the Certification Examination for Anti-Money Laundering Specialists (6th ed.). Miami, FL: ACAMS.

ComplyAdvantage. (2023)AML in Insurance: How to Detect & Combat Money Laundering 1. Retrieved from https://complyadvantage.com Financial Crime Academy. (2023)Anti Money Laundering (AML) In Insurance Industry In 2021 2. Retrieved from https://financialcrimeacademy.org

NEW QUESTION: 88

□ □□□ □□□□□□(FIU)□ □□□□ □□□□□□ □□□ SAR□ □□□□. FIU□ □ □□□ □□ FIU□ □□□□□□ □□□.

FIU □ □□□ □□ □□□ □□□□ □□ □□□□□□ □□□□□?

A. □□□□□□□□□(MLAT)

B. □□□□□ □□ □

C. □□□ □□□□□□□

D. □□ □□ □□

Answer: B (LEAVE A REPLY)

FIUs exchange information through secure platforms to investigate financial crime cases.

Option B (Correct): The Egmont Secure Web is the primary communication platform for FIUs globally.

Option A (Incorrect): MLATs allow for formal legal cooperation but are not an FIU-to-FIU communication tool.

Option C (Incorrect): INTERPOL databases track criminal records, not financial intelligence data.

Option D (Incorrect): The UN Sanctions List provides entity restrictions, not an FIU data-sharing mechanism.

NEW QUESTION: 89

□□ □□□ □□□ □ □□ □□□ □□□□ □□ □□□ □□□□□?

A. □ □□ □□

B. □□□ □□□ □□ □□□ □□ □□ □□ □□

C. □□ □□, □□, □□ □ □□□

D. STR □□□ □□□□ □□□

Answer: C (LEAVE A REPLY)

these are the main factors that determine the inherent money laundering risk of a financial institution. The customer base, location, products and services of a financial institution affect the type, volume, and complexity of transactions that it processes, as well as the exposure to high-risk customers, jurisdictions, and activities12. A financial institution should review these factors regularly and conduct a comprehensive risk assessment to identify, measure, and mitigate its money laundering risk34.

Reference:
Anti Money Laundering Risk Assessment - Financial Crime Academy1
Anti-Money-Laundering (AML) Risk Approach Explained | Okta2
Anti-Money Laundering (AML) Risk Assessment | ACAMS4
2024 National Money Laundering Risk Assessment (NMLRA)5

NEW QUESTION: 90
□□ □□□□□ □□□ □□ □□ □□ □□□□□□□□ □□□ □□□ □□□□□□?
A. Egmont □□□ □□ FIU □□
B. MLAT □□
C. Basel □□□□ □□ □□ □□
D. FATF □□
Answer: B (LEAVE A REPLY)
A commission rogatory, also known as a letter rogatory or a letter of request, is a formal request from a court in one country to a court in another country for some type of judicial assistance, such as service of process, taking of evidence, or enforcement of judgments1. A commission rogatory would be used in the context of a mutual legal assistance treaty (MLAT) request, which is a bilateral or multilateral agreement that enables countries to cooperate and provide legal assistance to each other in criminal matters2. MLATs are one of the main gateways for obtaining information from another country, especially when the information is not available through other means, such as financial intelligence units (FIUs), supervisory authorities, or international organizations3. FIUs are national agencies that collect, analyze, and disseminate financial information related to money laundering and terrorist financing, and they can exchange information with their counterparts in other countries under the Egmont principles. Supervisory authorities are regulators that oversee the compliance of financial institutions and other entities with anti-money laundering and counter-terrorism financing (AML/CFT) obligations, and they can share information with their peers in other jurisdictions through supervisory channels, such as the Basel Committee on Banking Supervision. The Financial Action Task Force (FATF) is an inter-governmental body that sets standards and monitors the implementation of AML/CFT measures, and it can provide information and guidance to its members and other jurisdictions, but it does not have the authority to request or compel information from them.
Reference:
1: Letters rogatory - Wikipedia
2: Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges | Federal Judicial Center
3: How US Authorities Obtain Foreign Evidence in Cross-Border Investigations | Global Investigations Review
: What is an FIU? | Egmont Group of Financial Intelligence Units
: Basel Committee on Banking Supervision | Bank for International Settlements
: What is the FATF? | FATF

NEW QUESTION: 91
□□□□ AML □□□□□□ □□□ □ □□□□□ □□ □□ □ □□□ □□□ □□□□.
A. □□□ □□ □□ AML □□□□ □□□□□□□.
B. □□ □□□□□ □□□□ □ □□ □□□ □□□□.
C. □□ □□ □□□□□□ □□□□□ □□□□□□ □□□□□.
D. AML □□ □□□ □□□ □3□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The Board of Directors is the primary governing body of a financial institution and has the fiduciary duty to oversee and approve the BSA/AML compliance program. One of the key responsibilities of the Board is to ensure the appointment of a qualified chief AML officer who has the authority, expertise, and resources to implement and manage the BSA/AML program effectively. The chief AML officer is accountable to the Board and senior management for the performance of the BSA/AML program and should report regularly on the status, issues, and challenges of the program. The Board should also evaluate the chief AML officer's performance and provide feedback and guidance as needed.
Reference:
The Board's Role in AML Compliance
Board Member Responsibilities for BSA/AML Compliance
Responsibilities of the Board of Directors in Implementing a Successful AML Program

NEW QUESTION: 92
□□ □□(FI)□ □□□ □□□□□ □□□ □□□□□ □□□ □ □□ □□□ □□□ □□□?
A. □□ □□□ □□□ □□ □□□□□ □□□□□ □□□□□ □□□.
B. □□□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□ □□ □□□ □□ □□□□□.
D. □□□ □□□□ □□ □□ □□ □□□□ □□□□.
Answer: (SHOW ANSWER)
FIs must handle law enforcement subpoenas carefully to comply with legal and AML obligations.
Option A (Correct): Legal counsel must review subpoenas to ensure compliance with AML and privacy laws.
Option B (Incorrect): Original documents should only be provided under specific legal conditions.
Option C (Incorrect): Account closure decisions must follow AML risk-based assessment.
Option D (Incorrect): Tipping off a customer about an investigation is illegal under AML laws.

NEW QUESTION: 93

Basel □□□ □□ □□□□□ □□□ □□□ □□□ □□□□□ □□ □□ □□□□□ □□□□□ □□□ □ □□□? (3□□ □□□□□□.)

A. □□□

B. □□□

C. □□□□□ □□□

D. □□

E. □□□

F. □□□/□□□

Answer: (SHOW ANSWER)

According to the Basel guidelines on customer due diligence for banks, a trust is a legal arrangement whereby a person (the settlor or grantor) transfers the legal ownership of specific assets to another person or entity (the trustee) to hold for the benefit of a third person or persons (the beneficiaries)1. The Basel guidelines recommend that banks should identify and verify the identity of the following parties to determine the true nature of the trust relationship:

The trustee, who is the person or entity that has the legal authority and duty to manage the trust assets and distribute them to the beneficiaries according to the trust deed2. The trustee may also be the settlor, the beneficiary, or both, depending on the type and structure of the trust3.

The beneficiaries, who are the persons or entities that have a beneficial interest in the trust assets or income, either presently or in the future4. The beneficiaries may be named individuals, classes of persons, or charitable causes.

The settlor or grantor, who is the person or entity that creates the trust and transfers the legal ownership of the assets to the trustee. The settlor or grantor may also retain some rights or powers over the trust, such as the ability to appoint or remove trustees, beneficiaries, or protectors.

The other three options are incorrect because:

Respondents are not trust parties, but rather financial institutions that maintain correspondent banking relationships with other financial institutions. Respondents are not relevant for the identification of the trust relationship, but rather for the due diligence of the correspondent banking relationship.

Payees are not trust parties, but rather persons or entities that receive payments from the trust or other sources. Payees are not relevant for the identification of the trust relationship, but rather for the monitoring of the transactions and activities of the trust.

Trust administrators are not trust parties, but rather persons or entities that provide administrative services to the trust, such as accounting, record-keeping, or tax compliance. Trust administrators are not relevant for the identification of the trust relationship, but rather for the assessment of the risk and complexity of the trust.

Reference:

1: Basel Committee on Banking Supervision, Customer due diligence for banks, October 2001, 4, p. 17 2: Basel Committee on Banking Supervision, Customer due diligence for banks, October

2001, 4, p. 17 3: ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 111 4: Basel Committee on Banking Supervision, Customer due diligence for banks, October 2001, 4, p. 17 : ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 111 : Basel Committee on Banking Supervision, Customer due diligence for banks, October 2001, 4, p. 17 : ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 111 : Basel Committee on Banking Supervision, Customer due diligence for banks, October 2001, 4, p. 10 : ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 112 : ACAMS, CAMS Study Guide, 6th Edition, Chapter 5, p. 112

NEW QUESTION: 94
A □□□ □□ □□ □□ □□□ □□ □□ □□□□ □ □□□□ □ □ □□ □□□ □□□ □□□ □□ □ □ □□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□□. □□ □ □ □□□□ □□□□ □□□ □□□□ □□□ □□ □□□□ □□□□□. □□ □□ □□□□ □ □□ □□ □□ □□□□ □□□ □□ □□ □□□ □□□ □□ B □□□ □□□□ □□□ □□□ □□ □□□□□ □□ □□ □□□□ □□□□□□.
□□ □□ □□□□ □□□ □□ □□□?
A. □□ □□
B. □□□□□□□□ □□□□ □□
C. □□□ □□□□□□□ □□□□□ □□□ □□□□ □□□□ □□
D. □□ □□ □ □□ □□ □□□□ □□□ □□□□ □□□□ □ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The junior account manager should file a suspicious transaction report (STR) with the Financial Intelligence Unit (FIU) of Country A, as he has reasonable grounds to suspect that the customer is involved in money laundering or terrorist financing. The customer's attempt to deposit a large sum of cash, followed by a series of smaller wire transfers from a high-risk jurisdiction, indicates a possible case of structuring or smurfing, which are techniques used by criminals to avoid detection and reporting thresholds. The junior account manager should not close the account, as this could alert the customer and disrupt the investigation by the FIU or law enforcement. The junior account manager should also not notify the anti-money laundering specialist of his bank, as this could create a conflict of interest or breach of confidentiality, unless the bank's policy requires such notification. The junior account manager should also not offer the customer a more secure method of depositing, as this could be seen as facilitating or condoning the customer's illicit activities, or exposing the bank to legal or reputational risks.
Reference:
CAMS Study Guide, pages 97-98, 103-104, 107-108.
CAMS Exam Questions and Free Practice Test, Question 272.

NEW QUESTION: 95
□□ □□ □□□ □□□ □□□ □□ □□ □□□□ □□ □□ □□□□ □□□ □□□□ □□□.
A. □□ □ □ □□ □□□□ □□□□□□□ □□ □□□□ □□□□ □□□□□ □□□.
B. □□ □□ □□□ □□ □□ □□ □ □ □□ □□□ □□□□□ □□□□□□.
C. □□ □□ □□□ □□ □□ □□ □ □ □□ □□□ □□□□□.

D. □□ □ □ □□ □□□□ □□□□□□□□ □□□□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
A compliance officer should communicate with regulatory and law enforcement authorities in line with applicable local laws during an ongoing investigation into a client's activities by a competent authority. This is because the compliance officer has a duty to cooperate with the authorities and provide relevant information and documents as requested, while also protecting the confidentiality and privacy of the client and the institution. The compliance officer should not restrict the communication to senior management only, as this could hinder the investigation or create a perception of obstruction. The compliance officer should not communicate only in writing, as this could limit the effectiveness and timeliness of the communication. The compliance officer should not limit the communication to the absolute minimum, as this could imply a lack of cooperation or transparency.
Reference:
CAMS Certification Package - 6th Edition | ACAMS1
CAMS Certifications: How to Get CAMS Certified | ACAMS2
ACAMS CAMS Certification Video Training Course - Exam-Labs3
Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)4

NEW QUESTION: 96
□□ □□ □ □□ □□ □□□ □□□□ □□□□□□ □□ □ □□ □□□ □□□ □□□□? 3□□ □□□ □□□□□□
A. □□□□□□ □ □□□ □□□ □□ □□□ □□□ □□ □ □□
B. □□□□□□ □□□ □□□ □□ □□ □□□□□ □□□ □□ □□, □□ □□ □□ □□□ □□□ □□□
C. □□□□□□ □□ □□□□ □□□□□
D. □□□ FIU□ □□
Answer: A,B,D (LEAVE A REPLY)
Havens for money laundering and terrorist financing are jurisdictions that offer a high degree of anonymity, secrecy, and protection to criminals who seek to conceal or move their illicit funds. These havens typically have the following three attributes12:
Limited types of institutions and persons covered by money laundering laws and regulations. This means that only a narrow range of financial activities or entities are subject to anti-money laundering (AML) and combatting the financing of terrorism (CFT) obligations, such as customer due diligence, record-keeping, reporting, and supervision. For example, some havens may exclude lawyers, accountants, trust and company service providers, or non-bank financial institutions from AML/CFT requirements.
Little enforcement of the laws, weak penalties or provisions that make it difficult to confiscate or freeze assets related to money laundering. This means that the authorities in these havens lack the political will, resources, or capacity to effectively implement and enforce the AML/CFT laws and regulations. They may also impose low sanctions or fines for non-compliance, or create legal

barriers or obstacles for the confiscation or freezing of assets that are the proceeds of, or used in, or intended or allocated for use in, money laundering, terrorist financing, or other crimes.
Absence of an effective FIU. This means that these havens do not have a central agency that is responsible for receiving, analyzing, and disseminating financial intelligence related to money laundering, terrorist financing, and other crimes. An effective FIU is essential for facilitating domestic and international cooperation and information exchange, as well as for supporting investigations and prosecutions of money laundering and terrorist financing cases.
Reference:
1: The IMF and the Fight Against Money Laundering and Terrorism Financing, 1 2: IX Special Recommendations, 2

NEW QUESTION: 97
□□ □□□ □□□ □□ □□ □□□ □□□ □□ □ □□ □□□ □□□□□? (2□□ □□□□ □.)
A. □ □□ □□ □ □□ □□□ □□□ □□□ □□ □□□ □□□□ □ □□□ □□□.
B. □□ □□□ □□□ □□□ □□□□ □□ □□ □ □□ □□ □ □□ □□□ □□ □□□ □□ □□ □□□.
C. □ □□ □□ □ □□ □□□ □□ □□□ □ □□ □□□ □□ □□□□ □□□□ □□□ □ □ □□ □□□□ □□□.
D. □ □□ □□ □ □□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□□ □□ □ □□ □□□ □□□□□ □ □□□.
Answer: A,C (LEAVE A REPLY)
A money laundering investigation that involves multiple countries can be challenging due to different legal systems, languages, cultures, and levels of cooperation. Two factors that can assist such an investigation are:
Law enforcement and other authorities should have access to financial information that is pertinent to the investigation. This can help them trace the flow of illicit funds, identify the perpetrators and beneficiaries, and gather evidence for prosecution. Financial information can be obtained from various sources, such as financial institutions, financial intelligence units, regulators, and international organizations.
Law enforcement and other authorities should be allowed to establish and utilize joint investigative teams with law enforcement in other countries. This can enhance coordination, communication, and information sharing among the authorities involved, and allow them to pool resources, expertise, and evidence. Joint investigative teams can also facilitate mutual legal assistance and extradition requests.
Reference:
Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations, February 2012, updated June 2019, Recommendation 40, pp. 120-123 FATF, Best Practices on Establishing and Operating a Joint Investigative Team, June 2020, pp. 5-6 FATF, Money Laundering and Terrorist Financing Investigations, June 2018, pp. 11-12

NEW QUESTION: 98
□□ □ □□□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□ □ □□ □□ □□□ □□ □□□?
A. □□□ □□□□□□□ □□□□□□□□ □□□□.
B. □□ □□□ □□□ □□ □□□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
According to the BSA/AML Manual1, once a financial institution files a SAR, it should maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. The supporting documentation should be identified and maintained by the financial institution as such, and be deemed to have been filed with the SAR. The financial institution should make all supporting documentation available to FinCEN or any federal, state, or local law enforcement agency, or any federal regulatory authority that examines the financial institution for compliance with the BSA, upon request. Therefore, the best action to take regarding a particular account once suspicious activity is reported by the institution is to secure all supporting documentation, as it may be needed for further investigation or examination.
Reference:
BSA/AML Manual1
Suspicious Activity Reporting - Overview2
Suspicious Activity Report (SAR) Basics3

NEW QUESTION: 99
□ □□□ $15,000 □□□ □□ □□□□ □□□ □□□ □□□ □□□. □□□ □□□ □□ □□ □□□□ □□ □□ □3□□□ □□□□ □□ □□□ □□□□□.
□□ □□□ □□□□ □ □□ □□ □□□ □□□□□? (2□□ □□□□□.)
A. □□ □□ □□ □□□□ □□
B. □□□□ □ □□□ □□ □□□
C. $15,000 □□□ □□ □□□□ □□□□
D. □□□□ □3□□□ □□□□□ □□□□ □□
Answer: (SHOW ANSWER)
Bringing $15,000 worth of chips into the casino is a red flag because it could indicate that the customer is trying to avoid the currency transaction reporting (CTR) requirement for cash transactions over $10,0001. Requesting a wire transfer to an unrelated third party is another red flag because it could indicate that the customer is trying to conceal the source or destination of the funds, or transfer them to a high-risk jurisdiction2.
Reference:
1: ACAMS CAMS Certification Video Training Course, Module 3: Casinos and Gaming, Section 3.1: Regulatory Requirements, Slide 8 2: ACAMS CAMS Certification Video Training Course,

Module 3: Casinos and Gaming, Section 3.2: Money Laundering Methods and Red Flags, Slide 11

NEW QUESTION: 100

□□ □□ □□□ □□□ □□□□□□ □□ □□□ □□ Wolfsberg □□ □□ □□ □□□ □□ □ □ □□□ □□□□ □ □□ □□□ □□□□□? (2□□ □□□□□.)

A. □□□ Financial Action Task Force □□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □ □□□□.

B. □□□ □□□□□□□□□(Financial Action Task Force) □□□□ □□□□ □□□ □□□ □ □□□ □□□□ □□□□□ □□□ □□□□□.

C. □□□ Financial Action Task Force □□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□ □□ □□□□□.

D. □□□ □□ □□ □□□□□ □□□□□ □□□ □□ □□ □□□ □□□□ □□ □□□□ □ □□□ □□□□□.

Answer: B,D (LEAVE A REPLY)

According to the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking, the risk of a correspondent bank customer depends on various factors, such as the nature of the customer's business, the customer's location, the products and services offered, the customer's ownership and management structure, and the customer's customer base1. Among these factors, two that should increase the risk and require additional due diligence are:

The customer is located in a Financial Action Task Force (FATF) member country and the bank's head of information security is a politically exposed person (PEP). A PEP is an individual who is or has been entrusted with a prominent public function, such as a senior government official, a judicial or military officer, a senior executive of a state-owned corporation, or a political party leader2. PEPs pose a higher risk of money laundering, corruption, or bribery due to their influence and access to public funds3. Therefore, a correspondent bank customer that has a PEP in a key position should be subject to enhanced due diligence, such as verifying the source of funds, the purpose of the relationship, and the PEP's reputation and integrity4.

The customer is located in a non-FATF member country and services mostly commercial customers who engage in international trade. A non-FATF member country is a country that is not part of the FATF, an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system5. Non-FATF member countries may have weaker or less consistent anti-money laundering and counter-terrorist financing regimes, and may pose a higher risk of financial crime or sanctions evasion6. Moreover, a correspondent bank customer that services mostly commercial customers who engage in international trade may be exposed to trade-based money laundering, which is the process of disguising the proceeds of crime and moving value through the use of trade transactions7. Therefore, a correspondent bank customer that operates in a non-FATF member country and deals with international trade should be subject to enhanced due diligence, such as obtaining information on the nature and volume of the trade transactions, the origin and destination of the goods, and the identity and reputation of the trade counterparties8.

The other options are not correct because they do not necessarily increase the risk of a correspondent bank customer or require additional due diligence. A customer that is located in a FATF member country and provides services primarily to a local individual customer may pose a lower risk of money laundering or terrorist financing, as the customer's activities are subject to the FATF standards and recommendations, and the customer's customer base is less likely to involve complex or cross-border transactions. A customer that is located in a FATF member country and provides services to other correspondent banks in neighboring countries may also pose a lower risk of money laundering or terrorist financing, as the customer's activities are subject to the FATF standards and recommendations, and the customer's customer base is composed of regulated financial institutions that are subject to their own anti-money laundering and counter-terrorist financing obligations.

nswer: BD

According to the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking, the risk of a correspondent bank customer depends on various factors, such as the nature of the customer's business, the customer's location, the products and services offered, the customer's ownership and management structure, and the customer's customer base1. Among these factors, two that should increase the risk and require additional due diligence are:

The customer is located in a Financial Action Task Force (FATF) member country and the bank's head of information security is a politically exposed person (PEP). A PEP is an individual who is or has been entrusted with a prominent public function, such as a senior government official, a judicial or military officer, a senior executive of a state-owned corporation, or a political party leader2. PEPs pose a higher risk of money laundering, corruption, or bribery due to their influence and access to public funds3. Therefore, a correspondent bank customer that has a PEP in a key position should be subject to enhanced due diligence, such as verifying the source of funds, the purpose of the relationship, and the PEP's reputation and integrity4.

The customer is located in a non-FATF member country and services mostly commercial customers who engage in international trade. A non-FATF member country is a country that is not part of the FATF, an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system5. Non-FATF member countries may have weaker or less consistent anti-money laundering and counter-terrorist financing regimes, and may pose a higher risk of financial crime or sanctions evasion6. Moreover, a correspondent bank customer that services mostly commercial customers who engage in international trade may be exposed to trade-based money laundering, which is the process of disguising the proceeds of crime and moving value through the use of trade transactions7. Therefore, a correspondent bank customer that operates in a non-FATF member country and deals with international trade should be subject to enhanced due diligence, such as obtaining information on the nature and volume of the trade transactions, the origin and destination of the goods, and the identity and reputation of the trade counterparties8.

NEW QUESTION: 101

□□ □□□ □□ □□□□□ □□□ □□□□□ □ □□□ □□ □□ □□□ □□ □□□ □□□□□ □ □□□. □□□ □□□□□ □□□□□□ □□□□□□□□□□ 2□ □□□ □□□□□ □□□□□ □□□ □ □□ □□□□□ □□□□□ □□ □□□□□□. □□ □□□□□ □□□ □□□□□ □ □□ □□□ □□□ □□□□□□?

A. □□ □□□ □□ □□□ □□ □□ □□□□□ □□□□□ □□ □□□ □□□□□ □□ □□□ □□ □□.

B. □□□ □□□ □□□ □□ □□□□□ □□□ □□ □□□ 2□ □□ □□□ □□□□□.

C. □□ □□□ □□□ □□ □□□ □□ □□□ □□□□□ □□□□□ □□□□□ □□□□□ □□□□□ □□□□□□.

D. 2□ □□□ □□ □ □□ □□□ □□ □□□ □□ □□□□□ □□□□□ □□□.

Answer: (SHOW ANSWER)

The threat of US sanctions against foreign individuals and entities continues to exist despite the absence of a US nexus. This is stated in the Certified Anti-Money Laundering Specialist (the 6th edition) manual on page 591, which states: "It is important to note that the threat of US sanctions against foreign individuals and entities continues to exist even when there is no direct US nexus (i.e., no US persons or assets involved)."

NEW QUESTION: 102

□□□□□□□□(Office of Foreign Assets Control) □□ □□□ □□ □□□ □□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□.

A. □□□ □□□□□ □□□.

B. □□ □□□□□□ □□ □□□.

C. □□□ □□□ □□□□□□□.

D. □□ □□ □□ □□.

Answer: B (LEAVE A REPLY)

The Office of Foreign Assets Control (OFAC) is the U.S. Treasury Department's agency that administers and enforces economic sanctions programs against countries, groups, and individuals that pose a threat to the national security, foreign policy, or economy of the U.S. OFAC's requirements have an extraterritorial reach because they apply not only to U.S. persons (citizens, permanent residents, entities, and those physically present in the U.S.), but also to any person or entity that engages in a transaction that has a connection to the U.S., such as using the U.S. financial system, U.S. goods, or U.S. persons. This means that intermediaries of a transaction with a U.S. nexus, such as foreign banks, brokers, or agents, are required to comply with OFAC's regulations and may face penalties for violating them. OFAC's jurisdiction does not depend on the registration or incorporation of an entity in the U.S., nor does it extend to foreign financial intelligence units, unless they are involved in a transaction with a U.S. nexus.

Reference:

The Aggressive Extraterritorial Reach of U.S. Economic Sanctions: Foreign Company Exposure to OFAC Enforcement OFAC Consolidated Frequently Asked Questions The global reach of OFAC sanctions Which three circumstances are U.S. banks required to block transactions?

NEW QUESTION: 103

□□□□ □□□ □□ □□□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□ □□ □□□ □ □□ □□□ □□□□□? 3□□ □□□ □□□□□

A. □□□□□□□ □□□ □□□ □□□ □□□ □□□ □□□□ □

B. □□□□□□ □□□□□□ □□□ □□□□□□ □□□□ □

C. □□□ □□□□□□□ □□□ □□ □

D. □□□□□□ □□□ □□(PEP)□□ □□□ □□

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

According to the Wolfsberg Principles on Private Banking, the bank should apply additional diligence to customers who present a higher risk of money laundering or other financial crimes. Some of the indicators for defining such customers are:

Persons residing in or having funds from countries with inadequate AML standards, sanctions, embargoes, or other measures that indicate a higher risk of money laundering or terrorist financing12.

Persons engaged in business activities known to be susceptible to money laundering, such as cash-intensive businesses, gambling, arms trade, precious metals and stones, art and antiquities, etc13.

Persons determined to be Politically Exposed Persons (PEPs), who are individuals who hold or have held positions of public trust or influence, or their family members or close associates, and who may pose a higher risk of corruption, bribery, or abuse of power14.

Persons who receive funds from a correspondent banking relationship are not necessarily required additional diligence, unless they fall under any of the above categories or other risk factors. Correspondent banking is a service provided by one bank to another bank to facilitate cross-border transactions, and it is subject to its own set of AML standards and due diligence measures5.

Reference:

Wolfsberg Anti-Money Laundering Principles for Private Banking (2012) 1 FATF High-Risk and Other Monitored Jurisdictions FATF Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22) FATF Guidance on Correspondent Banking Services

NEW QUESTION: 104

□□ □□□ □ □□□□ □□ □□□ □□□ □□□□□ □□, □□ □□ □□□□□ □□□□ □ □□□□ □□ □□□□ □□□ □□ □□□ □□□□□.

□□□□□□□ □□□ □□□□ □□ □□□ □□ □□□?

A. □□□□□ □□□□□□□□□□ □□□□□.

B. □□□□□ □□□□□□□□□ □□□ □□□□□.

C. □□□□□□□□ □□□ □□ □□□□ □□□ □□□.

D. □□□□□□□□□ □□□ □□□ □ □□□ □□□□ □□ □□□□ □□□□□ □□□□□.

Answer: B (LEAVE A REPLY)

be provided

Explanation:

Suspicious transaction report (STR) information is confidential and should not be disclosed to anyone outside the compliance function or law enforcement authorities. Providing STR information to the credit department could compromise the integrity of the reporting process and expose the institution to legal risks. The compliance officer should decline to provide the STR information to the credit department and explain the reasons for doing so.

Reference:

CAMS Certification Package - 6th Edition | ACAMS, Chapter 4: Conducting and Supporting the Investigation Process, page 136 CAMS Certifications: How to Get CAMS Certified | ACAMS, Candidate Handbook, page 16 ACAMS CAMS Certification Video Training Course - Exam-Labs, Video 4.3: Suspicious Transaction Reporting Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition), Practice Test 1,

NEW QUESTION: 105

□□ □ □□□□□ □□□ □□□?

A. □□

B. □□□

C. □□ □□

D. □□

Answer: D (LEAVE A REPLY)

According to the CAMS study guide, chapter 1, page 91, placement is the first stage of money laundering, where the illicit funds are introduced into the financial system. This stage involves the highest risk of detection, as the money launderers may use various methods to avoid suspicion, such as structuring, commingling, or using cash-intensive businesses. Placement is followed by layering and integration, which are the second and third stages of money laundering, where the illicit funds are moved and disguised through multiple transactions and entities, and then integrated into the legitimate economy as seemingly legal assets.

The other options are not the financial stages of money laundering, although they may be related to some aspects or techniques of money laundering. Option A, integration, is the final stage of money laundering, not the first. Option B, structuring, is a method of placement, not a stage of money laundering. Structuring, also known as smurfing, is the practice of breaking down large amounts of cash into smaller deposits or transactions to avoid reporting thresholds or scrutiny. Option C, off shoring, is a term that refers to the relocation of assets or activities to another jurisdiction, usually for tax or regulatory advantages. Off shoring may be used by money launderers to exploit the differences or loopholes between jurisdictions, but it is not a stage of money laundering.

Reference:

1: ACAMS CAMS Study Guide - 6th Edition, Chapter 1, page 9: https://www.acams.org/wp-content/uploads/2019/09/ACAMS-CAMS-Study-Guide-6th-Edition-Chapter-1.pdf

NEW QUESTION: 106

FATF□ □□ □□□ 2000-2001□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□□□ □□□ □ □□□□? 3□□ □□□ □□□□□

A. □□□ □□ □□ □□□

B. □□□ □□

C. □□□ □□□□ □□□□□ □□ □□

D. □□ □□ □□

Answer: (SHOW ANSWER)

According to the FATF typology report 2000-20011, lawyers can provide a range of functions that can be useful to a potential money launderer, such as:

Creating complex legal arrangements, such as trusts, foundations, or corporations, that can obscure the identity and ownership of the beneficial owners or the origin and destination of the funds.

Buying and selling property, such as real estate, art, or jewelry, that can be used to transfer or store illicit proceeds or to provide a legitimate cover for the source of funds.

Performing financial transactions on behalf of a client, such as opening bank accounts, transferring funds, issuing checks, or exchanging currencies, that can facilitate the movement or concealment of illicit funds.

Providing legal advice, on the other hand, is not a function that can be directly exploited by a money launderer, unless the advice is related to the above functions or to the avoidance or evasion of anti-money laundering laws and regulations.

Reference:

1: FATF Terrorist Financing Typologies Report - Financial Action Task Force2

NEW QUESTION: 107

□□ □□□ □□ □□ □□□ □□□□□?

A. □□ □□□ □□ □□□□□ □□□ □□□ □□□□□ □□□.

B. □□ □□□ □□ □□ □□□ □□□□□ □□□□□ □□ □□□ □□□□□.

C. □□ □□□ □□□□□ □□ □□ □□□ □□□□□□.

D. □□ □□□ □□□□ □□□ □□ □□□ □□□ □□□□□ □□ □□□□ □ □□ □□□ □ □□ □□□□ □□□□.

Answer: (SHOW ANSWER)

Funds transfers are electronic payments that move money from one account to another, either within the same financial institution or across different institutions, countries, or currencies1. Funds transfers are commonly used for legitimate purposes, such as remittances, trade, or investment, but they can also be abused by money launderers, terrorists, or fraudsters to move illicit funds or conceal their origin or destination2. Therefore, financial institutions and other entities that offer funds transfer services are required to apply anti-money laundering and counter-terrorism financing (AML/CFT) measures, such as customer due diligence, transaction monitoring, record-keeping, and reporting of suspicious activities2.

One of the red flags for funds transfers that may indicate money laundering or other criminal activity is when funds transfers are repeatedly sent to the same beneficiary out of line with the business purpose3. This could suggest that the originator and the beneficiary are colluding to layer or integrate illicit funds, or to evade reporting or sanctions requirements. For example, a business may send multiple funds transfers to the same supplier, but the amounts or frequencies do not match the invoices or contracts, or the supplier is located in a high-risk jurisdiction or is subject to sanctions. Alternatively, an individual may send frequent funds transfers to the same person, but the relationship or the reason for the transfers is unclear or inconsistent, or the person is associated with a criminal or terrorist organization. In such cases, the financial institution or the funds transfer service provider should conduct enhanced due diligence, verify the source and purpose of the funds, and report any suspicious activity to the relevant authorities.

Reference:

1: Wire Transfer Definition - Investopedia

2: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations | FATF

3: Wire Transfer Red Flags: Money Laundering & Fraud Risks - Alessa1

NEW QUESTION: 108

□□□ □□□□□ □□□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□ □ □□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□□□□?

A. □□ □□

B. □□ □□

C. □□□

D. □□ □□□□

Answer: (SHOW ANSWER)

Wash trading is the term for trading through multiple accounts, where an individual generates offsetting profits and losses and transfers of positions through accounts that do not appear to be commonly controlled. Wash trading is a form of market manipulation that creates artificial trading activity and volume, and may be used to evade taxes, inflate prices, or launder money. Wash trading can also involve the use of third parties or intermediaries to conceal the true identity and source of funds of the trader.

Reference:

The document titled "Money Laundering and Terrorist Financing Typologies and Trends in Canadian Securities Dealers" published by the Investment Industry Regulatory Organization of Canada (IIROC) in December 2019. You can access it by clicking here. This document states that "Wash trading is a form of market manipulation where an individual simultaneously sells and buys the same financial instruments to create misleading, artificial activity in the marketplace. Wash trading is illegal under securities law because it misleads investors and regulators about the true supply and demand of the securities involved. Wash trading can also be used to evade taxes, inflate prices, or launder money." The document titled "Market Manipulation" published by the Financial Industry Regulatory Authority (FINRA). You can access it by clicking here. This document states that "Wash sales are a form of market manipulation in which an investor simultaneously sells and buys the same security to create misleading, artificial activity in the marketplace. Wash sales are illegal under Section 9(a)(1)(A) of the Securities Exchange Act of 1934. Wash sales can be used to manipulate the price of a security, evade taxes, or launder money."

NEW QUESTION: 109

Egmont Group□ □□ □□□□□□ □□ □□□□□ □□□ □□□□□□ □□□ □□□□□□? (3□□ □□□□□□.)

A. □□□ □□□□□□ □□□ □□ □□ □ □□□ □□

B. □□ □□□ □□ □□ □□□□□ □□□ □□ □□

C. □□ □□□ □□ □ □□□□□□ □□□ □□ □□□□□ □□ □□□ □□□□□□.

D. □□ □□□□□□ □□□ □□ □□□□□ □□□□□□.

E. □□ □□ □□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□ □□□□□□.

F. □□□□□□ □ □□ □□ □□□□□□ □□□□□ □□□□□ □□ □□ □□□ □□ □□□ □□□ □□.

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

The Egmont Group assists financial intelligence unit members to accomplish their goals by providing support to expand and systematize cooperation related to the reciprocal exchange of information, fostering better and secure communication through the application of technology, and encouraging operational autonomy of financial intelligence units. Additionally, the Egmont Group also maintains uniform global formats for funds transfers that assist in the detection of money laundering and supplies information on the common money laundering tactics used by terrorists and financial supporters of terrorism.

NEW QUESTION: 110

□□ □ □□□□□□□ □□□□□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□□□?

A. □□ □□□

B. □□ □□□□□□ □□

C. Wolfsberg □□
D. □□ □□ □□□ □□
Answer: B (LEAVE A REPLY)
Financial Intelligence Units (FIUs) are the primary channels for sharing financial intelligence both within countries and across borders. FIUs cooperate with each other and other relevant law enforcement, regulatory, or intelligence agencies in the fight against money laundering, terrorism financing, and other financial crimes.

NEW QUESTION: 111
□ □□ □□□ □□ □□□□□ □□□□□□ □□□ □□ □□ □□□□□ □□□ □□□□□□ □□ □□□(STR)□ □□□□□ □□□□□. □ □, □□□ □□ □□□ □□□□□□.
□□□ □□□□□ □□ □□ □ □□ □□□ □□□ □□ □□ □□□ □□□ □ □□□□?
A. □□□ □□□ □□□ □□ STR□ □□□□□□□.
B. □□ □□ □□ □ □□ □□□
C. □□□□□ □□□□□ □□□ □□
D. □□□ STR □□ □ □□ □□
Answer: B (LEAVE A REPLY)
A law enforcement agency may request account opening documents and account statements from the institution to facilitate its investigation of a suspicious transaction report (STR). These documents can provide valuable information about the identity, background, source of funds, and transaction patterns of the customer, as well as any red flags or anomalies that may indicate money laundering or other criminal activities. Account opening documents may include identification documents, verification documents, customer due diligence forms, risk assessment forms, etc. Account statements may include transaction details, balances, fees, charges, etc.
Reference:
ACAMS, CAMS Examination Study Guide, 6th Edition, Chapter 4, pp. 115-116 FATF Guidance: The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing, October 20131, p. 20 Basel Committee on Banking Supervision, Sound management of risks related to money laundering and financing of terrorism, June 20172, p. 11

NEW QUESTION: 112
□□□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□□?
A. □□□ □□□□□□□□ □□□□□ □□ □ □□□ □□□□□ □□
B. □□□□□ □□ □ □□ □□□□□□ □□□ □□□ □□□□□ □□ □□□ □□
C. □□ □□□□□□ □□ □□□□□ □□□□□ □□ □□□ □□□ □□ □□□□□□.
D. □□□□□ □□□□, □□ □ □□□ □□□ □□ □□□ □□□ □□□□□ □□
Answer: (SHOW ANSWER)
The Black Market Peso Exchange (BMPE) is a trade-based money laundering technique commonly used by narcotics traffickers based in Colombia and Mexico. The central feature is the use of a money trader to ensure that the revenue from drug sales in the U.S. doesn't actually cross any borders. Instead, those dollars are used to purchase any number of legitimate

commodities from unsuspecting businesses on behalf of legitimate South American businesspersons, whose legitimate imports are used to obtain pesos for the drug cartels12. The BMPE involves six distinct steps:
Obtaining criminal proceeds: The drug cartels sell drugs for dollars in the U.S.
Involvement of intermediary services: The drug cartels sell the dollars to black market peso exchangers in Colombia at a discounted rate.
Identification of complicit companies: The black market peso exchangers identify exporting companies in the U.S. and importing companies in South America that are willing to participate in the scheme.
Placement of funds: The black market peso exchangers deposit the dollars into U.S. bank accounts or use money service businesses or other methods to transfer the funds.
Layering of funds: The black market peso exchangers use the funds to purchase monetary instruments such as checks, money orders, or wire transfers, or to pay for the goods ordered by the South American importers.
Integration of funds: The South American importers receive the goods or the monetary instruments and use them to pay for their imports or to sell them for pesos in the local market.
Reference:
1: Black Market Peso Exchange in Money Laundering - Financial Crime Academy
2: Overview - FinCEN.gov

NEW QUESTION: 113
□3□ □□ □□ □□ □□ □□□ □□ □□□ □□□□ □□□ □ □□ □□ □□□ □□□□□ □□□ □□(PEP)□□ □□□□ □□□ □□□?
A. 1□
B. 2□
C. 3□
D. 4□
Answer: B (LEAVE A REPLY)
According to the Third European Union Money Laundering Directive (3rd AMLD), a politically exposed person (PEP) is an individual who is or has been entrusted with prominent public functions, such as heads of state, government ministers, judges, senior military officers, or members of parliament1. The 3rd AMLD requires institutions and persons covered by the Directive to apply enhanced customer due diligence measures when dealing with PEPs residing in another Member State or in a third country, in order to prevent money laundering and terrorist financing risks1. The 3rd AMLD also specifies that a person who is no longer entrusted with a prominent public function shall not be considered a PEP after a period of at least one year has elapsed since that person left office, unless the institution or person covered by the Directive has knowledge or reason to believe that the person is still exposed to specific risks2. However, the Commission Directive 2006/70/EC, which lays down implementing measures for the 3rd AMLD, extends this period to at least two years, and allows Member States to extend it further, depending on the level of risk and the type of prominent public function involved3.

Reference:
1: Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
2: Article 3(8) of Directive 2005/60/EC
3: Article 2 of Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis

NEW QUESTION: 114
□□ □□□□□ □□□ □□ □□, □□ □□, □□ □□ □□ □ □□□ □□□ □□ □□□ □□ □ □□□□ □□□.
A. □□ □□ □□□ KYC □□□ □□□□□.
B. □□□ □□□ 3□□□□ □□□□□.
C. □□ □□□ □□□□□ □□□ □□ □□ □□□□□.
D. □□ □ □ □□ □□ □□ □□ □□□ □□□□□.
Answer: D ([LEAVE A REPLY])
The Basel Committee on Banking Supervision (BCBS) is an international body that sets standards and guidelines for the prudential regulation of banks. One of its key publications is the Customer Due Diligence for Banks, which outlines the essential elements of Know Your Customer (KYC) standards for banks. According to this document, customer acceptance, customer due diligence, and record-keeping policies and procedures should be changed as necessary to address variations in risk among each line of business within the organization. This means that banks should adopt a risk-based approach to KYC, taking into account the different types, levels, and sources of risk associated with different customers, products, services, transactions, and delivery channels. By doing so, banks can allocate their resources more efficiently and effectively, and mitigate the potential for money laundering, terrorist financing, and other financial crimes.
Reference:
Customer Due Diligence for Banks, BCBS, October 2001, p. 5, 14-15.
The Basel Committee: The Important Set Of International Banking Regulations, Financial Crime Academy, November 2023.

NEW QUESTION: 115
Egmont Group□ □□ □□□□ □□ □□ □□□□□?
A. □□□□ □□□□ □□
B. □□ □□□□□ □□ □□□□ □□ □ □□□
C. □□□ □□ □□□ □□ □ □□ □□ □ FIU□ □□ □□ □□ □□

D. □□ □□ □ □□ □□ □□□ □□□□ □□ □ □□□□□ □□□ □□□□ □□□ □□□ □
□□ FIU□ □□ □□

Answer: B ([LEAVE A REPLY])

The Egmont Group is a global network of Financial Intelligence Units (FIUs) that aims to enhance the capabilities and cooperation of its members in combating money laundering, terrorist financing, and other financial crimes. The Egmont Group supports its FIU members by helping them to expand and systematize the exchange of financial intelligence and information, improve expertise and capabilities of personnel, and enable secure communication with one another12.
The Egmont Group does not issue due diligence models for financial institutions, as this is the responsibility of national regulators and standard-setting bodies. The Egmont Group does not issue strategic products for law enforcement agencies and FIUs, as this is the role of other international organizations such as the Financial Action Task Force (FATF) and the United Nations Office on Drugs and Crime (UNODC). The Egmont Group does not expand the ability of FIUs to enforce laws and exchange information globally, as this depends on the legal and operational frameworks of each FIU and the bilateral or multilateral agreements they have with other FIUs.
Reference:
Egmont Group
Working Groups - Egmont Group
Overview of the Egmont Group of Financial Intelligence Units
The Egmont Group of Financial Intelligence Units | FinCEN.gov
Egmont Group - Qatar Financial Information Unit

NEW QUESTION: 116

□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ KYC □□□ □□□ □□□□ □□
□□.
□□ □ □□ □□ □□ □□□□□?
A. □□ □□□□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□□.
B. □□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□
□□□.
C. □□ □□ □□□□ □□ □□□□ □ □□ □□□ □□□ □□ □□□□ □□ □□□□□.
D. □□ □□□□ □□ □ □□□ □□ □□□□ □□ □□□ □□□ □□□ □□□□□.

Answer: ([SHOW ANSWER])

Money laundering risks arise when transaction patterns are inconsistent with a business's expected activity.
Option D (Correct): Multiple cash deposits in different branches is a known structuring (smurfing) technique, used to evade cash transaction reporting thresholds.
Option A (Incorrect): Depositing into both checking and savings accounts is normal behavior.
Option B (Incorrect): Irregular incoming payments may require further review but are not inherently suspicious.

Option C (Incorrect): Industry-related expenses (e.g., conference tickets) are normal business activity.

NEW QUESTION: 117

□□□ □□□□□ □□ □□□□□ □□ □□□ □ □□□ □□□□□□. □□ □□, □□ □□ □□□□□ □□□□□ □□ □□□ □□□□□□ □□□□□□ □ □□□□□□ □□□ □□□□□ □□□□□ □□□ □ □□□□. □□ □□□ □ □□□ □□□□ □□ □□□ □□ □□□□□□ □□□□□ □□□□.
□ □□□□□ □□□□□ □ □□□ □□ □□□□□ □□□ □□□□□□?

A. □□
B. □□
C. □□
D. □□ □□

Answer: C (LEAVE A REPLY)

The correct answer is C, as mapping scenarios are helpful in mitigating the weakness of not generating alerts when activity is consistently abnormal over a long period of time. Mapping scenarios are used to compare a customer's activity with their expected activity based on their profile, risk rating, or historical behavior1. By using mapping scenarios, the organization can identify customers whose activity deviates significantly from their normal or expected patterns, and flag them for further investigation. Mapping scenarios can also help detect changes in customer behavior over time, and alert the organization of any potential money laundering or terrorist financing risks.

NEW QUESTION: 118

□□□ □□□ □□□□□□ □□□□□□ □□□ □□□ □□□□□ □□□ □□□□□□?

A. □□□ □□ □□□□□ □□□□□ □□ □□□, □□□□□ □□□□□□□□ □□ □□□□□ □□ □□ □□ □□□□□□.
B. □□□ □□□ □□□ □□ □□ □□ □□□ □□□□□□ □□□□□□□□ □□ □□□ □□□ □□□ □□□□□□□□.
C. □ □ □ □□□ □□□ □□□ □□□□□ □□□ □□□ □□□□□ □□□ □□□□□ □□□□.
D. □□□ □□□□□ □□□□□ □□□□□ □□□ □□□ □□□□□ □□ □□□ □□□ □□□□□ □ □ □□ □□□ □□□□□□ □□□□□.

Answer: D (LEAVE A REPLY)

A beneficial owner is the natural person who ultimately owns or controls a legal entity or arrangement, such as a company, a trust, or a foundation. Identifying the beneficial owner is essential for preventing and detecting money laundering, terrorist financing, tax evasion, and other illicit activities that may involve the misuse of corporate vehicles. However, some individuals or entities may attempt to conceal the true beneficial ownership of a company by using various techniques, such as complex ownership structures, shell companies, bearer shares, or nominees. A nominee is a person or an entity that acts on behalf of another person or entity, usually for a fee or a commission, without disclosing the identity of the real owner or controller. Nominees can be used to protect or conceal the identity of the beneficial owner and controller of a company or asset. A nominee can help overcome jurisdictional controls on company ownership and circumvent directorship bans imposed by courts and government authorities. While the appointment of nominees is lawful in most countries, the use of nominees for money laundering purposes is illegal and a red flag for suspicious activity. Therefore, the person filling out an application on the company's behalf indicating that a beneficial owner is a nominee for another person not named in the company's documentation is an indicator that there is an attempt to conceal the company's true beneficial ownership12.

The other options are not necessarily indicators of concealment of beneficial ownership, as they may have legitimate explanations or reasons. The company having a subsidiary in another jurisdiction with a local investor as a beneficial owner may be a normal business practice or a strategic decision, as long as the ownership information is transparent and accurate. Recent changes to the company's ownership structure may reflect the company's growth, development, or adaptation to market conditions, as long as they are documented and reported to the relevant authorities. Beneficial ownership information from the time that the company was formed several years ago not matching the current information may be due to natural changes in the company's shareholders, directors, or managers, as long as they are updated and verified periodically.

Reference:

Concealment of Beneficial Ownership - Financial Action Task Force

What's a Beneficial Owner and Why Does it Matter? - Dun & Bradstreet

[ACAMS Study Guide, 6th Edition, Chapter 6, pp. 171-172]

NEW QUESTION: 119

□□ □□□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□□□.

A. □□□□□ □□ □□□□□.

B. □□□ □□□ □□□.

C. □□ □□ □□ □□□ □□□ □□□□.

D. □□ □□□□ □□□□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)

Bearer shares are unregistered equity securities owned by the possessor of the physical share documents. The issuing company does not record the identity or ownership of the shareholders, nor does it track the transfers of ownership. This means that the holder of the bearer share can claim ownership and exercise the rights associated with the share, such as voting and receiving dividends, by simply presenting the physical certificate. This also makes the transfer of ownership very easy, as it only requires the delivery of the physical document, without any formalities or intermediaries. Bearer shares are therefore attractive for those who seek anonymity, privacy, and flexibility in their corporate structures.

Reference:

Investopedia: Bearer Share

SuperMoney: Bearer Shares: Definition, Examples, and Implications

ACAMS: Bearer Shares

NEW QUESTION: 120
□□ □□ □□ □□□□□ □□□□□□ □□□ □□□ □□□□□ □□□ □□ □□□ □□□ □□□
□ □□ □□□ □□ □□□ □□□□□ □□□□.
□□ □□ □□□ □□□ □□□ □□□□□□?
A. □□□ □□
B. □□□□□
C. □□□□□□□ □□
D. □□□□□ □□□□□
Answer: B (LEAVE A REPLY)
A fundraising organization is a type of non-profit organization that may be vulnerable to money laundering and terrorist financing risks, as they often operate in high-risk areas, deal with large amounts of cash, and have complex and opaque structures. Therefore, a fundraising organization warrants enhanced due diligence, which is a higher level of customer verification and monitoring that goes beyond the standard customer due diligence measures. Enhanced due diligence may include obtaining additional information on the source of funds, the purpose of the relationship, the beneficiaries, and the governance of the organization.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 2: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Section 2.2: Customer Due Diligence, p. 33-34 Anti-money laundering - a guide to customer due diligence Customer due diligence | The Law Society

NEW QUESTION: 121
□□ □ □□ □□□ □□□□□□ □□□ □□ □□□ □□□ □□□ □□□ □□□□.
(2□□ □□□□□□.)
A. □□□ □□□□□ □□□□□ □□ □□□ □□ □□.
B. □□ □□□ □3□ □□□ □□□.
C. □□ □□□ □□ □□ □□ □□ □□.
D. □□ □□□ □□□□□□ □□ □□ □□ □□.
E. □□ □□□□□ □□□ □□ □□ □□.
Answer: A,C (LEAVE A REPLY)
This is stated in the Certified Anti-Money Laundering Specialist (the 6th edition) manual on page 595, which states: "Potential indicators of money laundering associated with Trust and Company Service Providers include the use of legal persons in jurisdictions with strict secrecy laws, structuring cash deposits into third party accounts, multi-jurisdictional wire transfers with no legal purpose, and frequent deposits to or withdrawals from bank accounts."

NEW QUESTION: 122

□□□ □□□ □□□ □□ □□□ 3□□□ □□□□□?

A. □□

B. □□□□

C. □□

D. □□□

Answer: A,B,C (LEAVE A REPLY)

Online banking is vulnerable to all three stages of money laundering, namely placement, layering, and integration, because it allows the movement of funds across different accounts, jurisdictions, and institutions with speed, anonymity, and convenience. Online banking can facilitate the following money laundering methods:

Placement: The initial stage of money laundering, where illicit funds are introduced into the financial system. Online banking can enable placement by allowing the deposit of cash or checks through ATMs, mobile devices, or remote deposit capture, or the transfer of funds from prepaid cards, digital wallets, or cryptocurrencies to bank accounts.

Layering: The second stage of money laundering, where illicit funds are moved, disguised, or concealed to obscure their origin and ownership. Online banking can enable layering by allowing the transfer of funds between multiple accounts, often in different jurisdictions or currencies, or the purchase of financial products or services, such as money orders, wire transfers, or online gambling, that create complex transaction trails.

Integration: The final stage of money laundering, where illicit funds are reintroduced into the legitimate economy as apparently legal income or assets. Online banking can enable integration by allowing the transfer of funds to legitimate businesses, investments, or charities, or the purchase of goods or services, such as real estate, luxury items, or travel, that provide a cover for the source of funds.

Reference:

ACAMS CAMS Certification Video Training Course1, Module 2: Money Laundering Risks and Methods, Lesson 2.1: The Three Stages of Money Laundering ACAMS CAMS Study Guide, 6th Edition2, Chapter 2: Money Laundering Risks and Methods, Section 2.1: The Three Stages of Money Laundering, pp. 29-34 ACAMS CAMS Examination Preparation Seminar, 6th Edition3, Chapter 2: Money Laundering Risks and Methods, Section 2.1: The Three Stages of Money Laundering, Slides 9-13

NEW QUESTION: 123

□□□□/□□□□□□ □□□ □□ FATF(Financial Action Task Force) □□□ □□□ □□ □□□ □□□□□?

A. □ □□□□ FATF □□□□ □□□ □□□□□ □□

B. □□ □□ □□ □□ □□
C. □□□ □ □□ □□ □□
D. FATF □□□ □ □□□ □□ □□
Answer: C (LEAVE A REPLY)
The FATF Regional Style Bodies (FSRBs) are autonomous regional organizations that help the FATF implement its global AML/CFT policy, which revolves around its 40 Recommendations, in over 200 affiliated countries1. One of the key characteristics of the FSRBs is that they emphasize regional co-operation between member countries, as stated in the High-Level Principles and Objectives approved by the FATF Plenary in October 20122. This means that the FSRBs facilitate information exchange, technical assistance, training, and mutual support among their members to enhance their AML/CFT capacities and compliance. The FSRBs also promote regional perspectives and specificities in the FATF policy-making process and foster dialogue and collaboration with other regional and international bodies2.
Reference:
1: What are the 9 FATF-Style Regional Bodies (FSRBs)? - Sygna
2: FATF-Style Regional Bodies (FSRBs) - Asia/Pacific Group on Money Laundering

NEW QUESTION: 124
□□ □□(FI) □□□ □□□ □□ □□ □□□ □□□□ □ □□ □□ □□□ □□□ □□□□.
A. 1□ □□□□ □□ □□□ □□□□□ □□□□ □□□.
B. □□ □□ □□ □□□ □□ □□□□ □□□□ □□□.
C. □□ □□□ □□ □□□ □□□□□ □□□.
D. □□ □□ □□□ □□□ □□□□ □□□□ □□□.
Answer: (SHOW ANSWER)
An enterprise-wide compliance culture is a centralized, coordinated approach to ethics and compliance program design and assessment that cuts across multiple business units within an organization1. One key aspect of promoting such a culture is that the relevant information should be shared throughout the organization, so that all employees are aware of the compliance risks, policies, procedures, and expectations, and can act accordingly2. Sharing information also facilitates collaboration, communication, and feedback among different functions and levels of the organization, and helps identify and address any gaps or issues in the compliance program3. By contrast, the other options are not conducive to an enterprise-wide compliance culture, as they either create silos, conflicts, or inefficiencies in the compliance function.
Reference:
1: Enterprise Compliance Risk Management Services | Deloitte US
2: Enterprise Risk Management and Risk Culture - McKinsey & Company
3: FRB: Speech, Bies-Enterprise-wide Compliance Programs-February 4, 2004

NEW QUESTION: 125
□□(□□) □□□□ □□□□ □□□□ □□□ □□□□ □□□□□ □□□□□ □□ □□ □□ □□□?

A. □□□□ □□□□ □□□□ □□
B. □□ □□□ □□□□ □□
C. □□□□ □□□□ □□□ □□□□□.
D. □□ □□□□ □□□□□ □□□□ □□
Answer: B (LEAVE A REPLY)
Reference:
"Who must comply with OFAC regulations?U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods. please refer to: https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions

NEW QUESTION: 126
Financial Action Task Force 40 Recommendations□ □□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□ □□ □□□?
A. □□□ □□□ □□ □□ □□
B. □□ □□□ □□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□□.
C. □□□ □□□ □□ □□□ □□ □□□□ □□□ □□ □□□ □□□□□ □□□□ □ □□□ □ □□□ □□□.
D. □□□ □□□ □□□ □□□□□ □□□□□□□ □□ □□ □□□□ □□ □□ □ □□□ □ □□□ □□ □□□□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
According to the Financial Action Task Force (FATF) 40 Recommendations, countries should implement measures to prevent the abuse of non-profit organizations (NPOs) for the financing of terrorism. One of these measures is to ensure that NPOs cannot be used to conceal or obscure the diversion of funds intended for legitimate purposes to terrorists' organizations. This means that countries should have effective mechanisms to monitor and supervise NPOs, especially those that are at risk of terrorist financing abuse, and to take appropriate actions against NPOs that are involved in such activities. Countries should also ensure that NPOs maintain adequate records of their activities and transactions, and that these records are accessible to competent authorities. Furthermore, countries should promote transparency and accountability in the NPO sector, and encourage NPOs to conduct due diligence on their donors, beneficiaries, and associates.
Reference:
FATF 40 Recommendations, Recommendation 8 and Interpretive Note to Recommendation 8
Best Practices on Combating the Abuse of Non-Profit Organisations, FATF, June 2015
COMBATING THE ABUSE OF NON-PROFIT ORGANISATIONS (RECOMMENDATION 8), FATF, June 2015

NEW QUESTION: 127
□□□□ □□□□ □□ □ □□□□□ □□ □□□ □ □ □□ □□ □□□□□? (2□□ □□□□ □.)
A. □□□□ □□□ □□ □□□□ □□□ □□□ □□□□.
B. □□□□ □□ □□□ □□□□ □□ □□□□□ □□□ □□□□□.
C. □□□□ □□ □□□□□ □□□ □□ □□□ □□□□□.
D. □□□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□□□.
E. □□□□ □□□ □□□□ □ □□□ □□□□□.
Answer: A,C (LEAVE A REPLY)
Lawyers who lack experience in providing specific services requested by clients or receive unusually high fees can raise red flags for money laundering. Inadequate documentation of case notes may also be suspicious, but the absence of experience and excessive fees are more significant indicators. These behaviors warrant further scrutiny to assess potential money laundering risks12.
Reference:
1. ComplyAdvantage: AML Red Flags - What are the Top 10 Indicators?
2. HyperVerge: AML Red Flags: A Guide to Identification and Response

NEW QUESTION: 128
□□□ □ □ □□ □□ □□ □□□ □□□ □□□ □□□□. □□ □□□ □□□□ □□□□□ □
□□ □□ □□ □□□□ □□□ □□□ □□□□□ □□□ □□□□□.
□□ □□□ □□ □ □□ □□ □□ □□□□ □□□□ □□□ □□□□□?
A. □□□□□ □□□□ □□□ □□ □□□□.
B. □□□□□ □□ □□□ □□□ □□ □□□□.
C. □□ □□□□ □□ □□ □□□ □□ □□ □□
D. □□□□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The charity frequently withdrawing cash from the bank indicates possible terrorist financing, as cash transactions are often used to conceal the source, destination, and purpose of funds. Cash transactions also make it difficult to trace the flow of funds and identify the beneficiaries. Terrorist financiers may use charities as a cover to collect and distribute funds for their activities, and may exploit the cash-based nature of charitable donations to avoid detection12.
Reference:
20Typologies%20Report.pdf

NEW QUESTION: 129
□□ □□ □□ □□ □□□ □□ □□□□□□□ □□□?
A. 2□□□
B. □□ □□ □□ □
C. □□□□ □□□□ □□
D. □□□□□□□ □□□ □□ □□

Answer: B (LEAVE A REPLY)
Evaluating the risk scoring model and conducting the risk assessment itself may need to be performed annually, every eighteen to twenty-four months, before the launch of a new product, or when an acquisition of another financial institution occurs.
Reference:
Assessment-FAQs-2015.pdf (10)

NEW QUESTION: 130
□□□ □□□ □□□ AML □□□ □□ □□ □□ □□□ □□□ □□ □□ □□□□□□□ □□□ □□ □□ □□□ □□ □□ □□□□□?
A. □□□□□□ □□
B. □□ □□
C. □□ □□ □□ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
According to the FATF Recommendations (2012), page 111, the FATF calls on its members and urges all jurisdictions to apply enhanced due diligence and, in the most serious cases, countermeasures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing risks emanating from countries with significant strategic AML/CFT deficiencies. Countermeasures are proportionate and effective actions that can be applied by countries individually or collectively to protect their financial systems from these risks. Examples of countermeasures include restricting or prohibiting financial transactions with the high-risk country, requiring financial institutions to review and terminate correspondent relationships with the high-risk country, or applying enhanced reporting mechanisms or systematic reporting of financial transactions with the high-risk country.
Reference:
FATF Recommendations (2012), page 111
FATF Public Statement on High-Risk Jurisdictions subject to a Call for Action, February 20232
FATF Guidance on Countermeasures, October 20103

NEW QUESTION: 131
□□ □□□□□□ □□□□□□ □□ □□ □□□□□□ □□ □□ □□□ □□□□ □□□□. □□ □ □□ □□□ □□□□□ □□□? (2□□ □□□□□.)
A. □□□ □□□ □□□ □□□□ □□□ □□□□ □□□ □□□□□.
B. □□□ □□□ □ □□□ □□□ □ □□□□.
C. □□□ □□□ □□□□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□ □□□□.
D. □□□ □□ □□ □3□□□ □□□ □□□ □□□□□.
E. □□□ □□ □□□ □ □□□ □□ □□□□□.
Answer: A,B (LEAVE A REPLY)
This information can be found in the Certified Anti-Money Laundering Specialist (CAMS) study guide, 6th edition, under the section on Unusual Customer Identification Scenarios. The guide

explains that two indicators that should be included in awareness training for unusual customer identification scenarios are:
A . The customer opens the account in the name of a family member who begins making large deposits.
This is an indicator of potential structuring, where a customer may be attempting to avoid triggering reporting thresholds by depositing funds in smaller amounts over time. It is important for staff to be aware of this scenario and to monitor accounts for potential suspicious activity.
B . The customer's name and home address cannot be verified.
This is an indicator of potential identity theft or other fraudulent activity. If a customer's identifying information cannot be verified, it is important for staff to conduct additional due diligence to ensure that the customer is legitimate and that the account is not being used for illicit purposes.

NEW QUESTION: 132
□□□□ □□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□ □□□□.
□□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□□□ □□□□ □□□ □□□.
B. □□□ □□ 5□ □□□ □□□□ □□ □□ □□□ □□□□□.
C. □□□□□□ □□□ □□□□ □□□□ □□ □□ □□□□ □□ □□ □□□ □□ □□□ □ □□ □□□□□.
D. □□□□□□ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□ □ □□□□ □□□□.
Answer: (SHOW ANSWER)
According to the risk-based approach, financial institutions should apply enhanced due diligence and ongoing monitoring to higher-risk clients, and take appropriate measures to mitigate the risks of money laundering and terrorist financing. If the client exceeds the criteria of an acceptable risk model created by the institution, the institution should communicate the issues to the client and request remedial actions, such as providing additional information, documentation, or evidence of compliance. If the client does not cooperate or comply with the institution's requirements, the institution should consider terminating the relationship with the client, as the risk may outweigh the benefits of continuing the business relationship.
Reference:
ACAMS CAMS Certification Package - 6th Edition, Chapter 2: Risk Assessments, pp. 51-521
ACAMS CAMS Certification Package - 6th Edition, Chapter 4: Customer Due Diligence, pp. 97-981 ACAMS CAMS Certification Video Training Course, Module 2: Risk Assessments, Lesson 2.3: Risk-Based Approach2 ACAMS CAMS Certification Video Training Course, Module 4: Customer Due Diligence, Lesson 4.3: Enhanced Due Diligence

NEW QUESTION: 133
□□□ □□□ □□ □□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□ □□ □ □ □□□□ □□□□ □□□□.
□□ □□□□ □□ □□□□□?

A. □□□ □□ □ □□□ □□ □ □□ □□□□
B. □□ □□ □ □□ □□
C. □□□□□□□□ □□ □□□□
D. □□ □□□□ □□□□ □□
Answer: B (LEAVE A REPLY)

Results of related audits and examinations are the most useful report for an anti-money laundering specialist to inform senior management about the status of the anti-money laundering program across the organization. This is because audits and examinations provide an independent and objective assessment of the effectiveness, efficiency, and compliance of the anti-money laundering program, as well as identify any gaps, weaknesses, or areas for improvement. Audits and examinations can also help senior management to monitor the performance of the anti-money laundering program, ensure accountability and oversight, and demonstrate commitment to regulatory expectations and best practices.

Reference:

Anti-Money Laundering Preparedness Survey Report 2020 - Deloitte US, page 4.

CAMS Study Guide 6th Edition, page 39.

NEW QUESTION: 134

STR □□□ □□□□ □□□ □ □□ □ □□□ □□□□ □□□?

A. □□ STR□ □□ □□
B. □□ STR□ □□ □□ □ PEP, □□ □□□ □□□ □□ STR □□
C. PEP □ □□ □□□ □□□ □□ □□ STR □□
D. □□ FIU□ □□□ □□ STR
Answer: B (LEAVE A REPLY)

In many jurisdictions, it is a requirement to report certain information regarding STRs to senior management and/or the board of directors. This information may be limited to the number of reports filed, the dollar amounts involved and significant trends as observed by compliance personnel. In some cases, if the activity presents a significant or potentially ongoing risk to the institution, the leaders of the institution should be made aware so that high-level decisions can be made regarding potential changes to systems, staffing, products, services or particular relationships maintained by the institution.

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties, while being mindful of the confidential nature of the SAR.

https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/0

NEW QUESTION: 135

□□□ □□ □□□□□ □□□ □□ □□ □□ □□ □□□□□□ □□□□□□□. □ □□□□□□ □□ □□□□ 30□ □□□ □□ □□□□□□ □□□□□ □□ □□□ □□□ □ □□□ □□□□□ □□ □ □ □□□□□□□ □□□□□ □□□□□. □□ □□□ □□ □ □□□ □□□ □□□ □□ □□ □□□ □□□□.
□□ 1□ □□ □□ □□ □□□ □□□ □□□ □□□□□ □□□□□ □□□□□ □□□□□□. □□ □ □ □□□□□ □□ □□ □□□ □□□ □□□□□ □□ □□□□□ □□ □□ □□□ □ □□□ □□□ □ □□□□□□ □□□.
□ □□ □□□ □□□□□ □□ □ □□ □□□ □□□ □□ □ □□□□? (2□□ □□□□□□.)

A. □□ □□□ □□, □□ □□ □□
B. □□□ □□□ □□ □□
C. □□ □□, □□ □ □□□□□□ □□
D. □□ □□□□□□ □□□□□□ □□□□□ □□□□□ □□

Answer: A,D (LEAVE A REPLY)

By delivering the same annual refresher training to all employees, the compliance officer could miss the opportunity to update the staff on any new trends, developments, or risks that have emerged in the anti-money laundering field. For example, new typologies, indicators, technologies, or best practices could be relevant for the staff to be aware of and apply in their daily work. Moreover, the compliance officer could also miss the chance to share any links to enforcement actions identifying violations in other financial institutions that could serve as lessons learned or case studies for the staff to avoid similar mistakes or gaps in their compliance program.
Reference:
ACAMS CAMS Certification Video Training Course, Module 5: Risk Management, Lesson 5.4: Training1 ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 5: Risk Management, Section 5.4: Training2

NEW QUESTION: 136

□□ □□ □□□□□ □□ □□ □□□ □□□ □ □□□ □□□□□ □□□ □□ □□□ □□□□□ □ □□□. □□□ □□ □□□ KYC □□□□□□ □□□□□ □□□ □□ □□□□□□?

A. □□□□□□ □□□ □□ □□□ □□
B. □□ □□□□□□ □□□ □□□ □□
C. □□□□□□□ □□□ □□□□□ □□□ □□ □□
D. □□□ □□□ □□ □□□□□□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

According to the Certified Anti-Money Laundering Specialist (CAMS) study guide, 6th edition, page 105, the correct answer is C. It can be difficult to determine if there is negative media associated with counterparties solely from the customer's account activity and KYC file.
The study guide explains that negative media can include news articles, government sanctions lists, and other sources of public information that may indicate that a counterparty is involved in

illicit activities. However, this information may not be readily available in a customer's account activity or KYC file, and may require additional research or investigation.

NEW QUESTION: 137

EU Trust and Company Service Provider(TCSP) □□□□□ □□□ □□□□□□ □□□ □□□□□□ □ □□□□□ □□ □ □□ □□□□□□ □□□ □□□□□□□. □□□ □□□ □□□□□ □□□□□ □ □□ □□ □□□□□. □□ □□ □□□ □□□□□□□□ □□□ □□□□□□□□□ □□□?

A. □□□□□□□ □□□□□ □□□□□ □□□□ □□□□□ □□ □□□□ □□.
B. □□ □□ □□□□ □□□□□ □□.
C. □□□□ □□□□ □□ □□ □□ □ □□□□ □□□□□ □□ □□□□ □□□□ □□
D. □□□□ □□□□□ □□ □□ □□□□ □□ □□ □□□□□ □□□□□□.

Answer: C (LEAVE A REPLY)

According to the CAMS Study Guide, one of the methods to launder money using TCSPs is to create a complex web of transactions involving multiple entities and jurisdictions, often using shell companies and nominees. The payment of consultancy fees to unrelated companies and service providers established in a foreign jurisdiction could be a sign of such a scheme, as it could be used to disguise the origin and destination of illicit funds, or to evade taxes and regulations. Therefore, this transaction indicator warrants further escalation to the compliance officer.

NEW QUESTION: 138

□□ □□□ □□□ □□□ □□□ □□ □□□□□ □□□ □□□ □□□□□ □□□ □□□ □□□ □□□□□ □□□?

A. 1□□ □□
B. □□ □□□
C. □□ □□ □□
D. □□ □□□

Answer: B (LEAVE A REPLY)

According to the Basel Committee guidelines, banks should formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk customers12. The customer acceptance policy should be approved by senior management and include clear guidelines on the types of customers that are likely to pose a higher than average risk to the bank1. Senior management should also ensure that the bank has adequate resources and systems to effectively manage the risks associated with higher risk customers1. Therefore, senior management should determine whether or not to enter business relationships with higher risk customers, based on the bank's risk appetite, policies, and procedures.

Reference:

CAMS Study Guide (the 6th edition), page 1843

Customer due diligence for banks - Bank for International Settlements1

The Basel Committee: The Important Set Of International Banking Regulations2

NEW QUESTION: 139

□□□ □□□ □ □□□□□□ □□□ □□□ □□□□ □ □□□□ □□ □□□ □□ □□□□ □ □□□ □□ □□ □□ □□□ □□□ □□□?

A. □□□ □□□ □□□ □□□ □□□ □□□ □□□□.

B. □□ □□□□□ □□ □□□□□ □□□□ □□□□ □□□□□□ □□□□□.

C. □□ □□□□□ □□□□□□ □□□ □ □□ □□□ □□□ □□□□□.

D. □□□ □□□ □□□□ □□□ □□□ □□□□□.

Answer: (SHOW ANSWER)

According to the ACAMS CAMS Certification Study Guide (6th edition), one of the key steps of conducting an investigation of a suspicious activity is to maintain and secure supporting documentation used to perform the investigation. This includes the transaction activity that generated the alert, the analysis performed, the decision made, and the rationale for the decision. This documentation serves as evidence of the investigation process and the compliance with the relevant policies and procedures. It also helps to ensure consistency, accountability, and transparency in the investigation process1

NEW QUESTION: 140

□□□ □□□□□ □□□□□□ □□ □□□□ □□ □□□□□□ □□□ □□□□ □ □□ □□ □□□□□ □□□ □□ □□□ □□□□□□□□ □□□ □□ □□□ □□□ □□□□ □□□. □□. □□□□□□ □□ □□ □□□□ □□□ □□□ □□ □□□ □□□ □□□□. □ □□□ □ □ □□ □□□ □ □□□ □□□□□□. □□□ □□□ □□ □□ □□□□ □□ □□ □□ □□□ □ □□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □ □□□□□. □□ □ □□□□□□ □□□ □□ □ □□ □□□□□?

A. □ □□□ □□□ □□ □□□ □□□□□ □□ □□□ □□□□□.

B. □□ □□□ □□□□ □□□□□ □□ □□□□ □□□ □□□□ □□□□□.

C. □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.

D. □□□ □□□□ □□□□ □□ □□□ □□□□ □□□□□.

Answer: C (LEAVE A REPLY)

According to the ACAMS CAMS Study Guide (the 6th edition), one of the key steps in conducting an effective investigation of a potential money laundering or terrorist financing activity is to gather all relevant information about the customer and the transaction, including the nature and purpose of the account, the source and destination of funds, the expected account activity, and the customer's risk profile1. In this case, the compliance officer should meet with the staff who

opened the new account for the public official to obtain this information and assess whether the account is consistent with the customer's profile and needs, or whether it indicates a possible attempt to conceal or launder illicit funds. Waiting for the new account to receive funds, calling the competent authorities, or calling the official's office are not appropriate actions at this stage, as they may compromise the investigation, alert the customer, or violate confidentiality rules1.
Reference:
ACAMS CAMS Study Guide (the 6th edition), Chapter 4: Conducting or Supporting the Investigation Process, page 1311

NEW QUESTION: 141
□□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□□□ □□□ □□□□
□. o □□ □□□□ □□□ □□□□□ □□ □□□ □□ □□□ □□□
A. □□□ □□□ □ □□ □□ □□□□□.
B. □□ □□ □□□ □□□□ □□□ □ □□□ □□□.
C. □□□□ □□□ □□ □□□ □□□□ □□□□ □□□□□ □□□□□.
D. □□□□ □□□□□ □□□□□ □□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
One of the main challenges and risks for online banks is the verification of customer identity and the prevention of identity fraud. Online banks are more vulnerable to money laundering and terrorist financing because they do not have face-to-face contact with their customers and may rely on third-party sources or digital methods to verify customer information. Therefore, the most important recommendation for the anti-money laundering expert to make is that the online bank ensures that prospective new customers can be properly identified and that their identity documents and information are verified using reliable and independent sources. This is also in line with the international standards and best practices for anti-money laundering and counter-terrorist financing, such as the FATF Recommendations, the Basel Committee on Banking Supervision principles, and the EU's Fifth Anti-Money Laundering Directive123 The other options are less important or less effective than ensuring customer identification. Limiting the amount that can be processed per transaction may reduce the exposure to large-scale money laundering, but it does not prevent the use of multiple transactions or accounts to launder smaller amounts. Setting up automated programs to analyze transactions for money laundering activity may enhance the detection and reporting of suspicious transactions, but it does not address the root cause of money laundering, which is the concealment of the source and ownership of illicit funds. Ensuring that a firewall is set up to protect the transactions may improve the security and confidentiality of the online banking system, but it does not prevent the misuse of the system by money launderers who have legitimate access to the system123 Reference:
1: Anti-Money Laundering Guide for Digital Banks by sanctions.io, 2022
2: The fight against money laundering: Machine learning is a game changer by McKinsey, 2021
3: FATF Guidance on Digital Identity, 2020

NEW QUESTION: 142

□□□ □□□□ □□□ □□ □□ □□□□ □□ □□ □□□ □□ □ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□ □□□□□□□.
□□ □□□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□ □ □□
B. □□ □□ □□□ □ □□□□ 1□□ □□□□
C. □□□ □□ □□□□ □□ □□□ □ □□ □□□□ □□□□
D. □□□□ □□ □□□□□□ □□□ □□ □□□ □□
Answer: (SHOW ANSWER)
Customer due diligence should be implemented as an ongoing activity that may vary commensurate with the risk profile of the customer. This is because the risk of money laundering or terrorist financing may change over time, depending on the customer's behavior, transactions, products, services, and geographic locations. The institution should monitor the customer's activity and update the customer's information and risk assessment periodically, or when there are red flags or significant changes in the customer's circumstances. The institution should also apply enhanced due diligence measures for customers that pose higher risks, and simplified due diligence measures for customers that pose lower risks12.
Reference:
1: CAMS Certification Package - 6th Edition | ACAMS, Chapter 1: Risks and Methods of Money Laundering and Terrorist Financing, p. 18-19 2: FATF Guidance: Customer Due Diligence and Financial Inclusion, February 2018, p. 10-11, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-CDD-and-Financial-Inclusion-2018.pdf

NEW QUESTION: 143
□□ □ □□□□ □□ □□□□□ □□ □□ □□ □□ □□□ □ □□□□ □□ □□□□ □□ □ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□□□□□ □□ □□□□ □□□ □□□□□ □□□□ □□ □□ □□□□ □□□□ □□□ □□ □□□□.
B. □□□ □□□□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□□ □□□□□.
C. □□□ Financial Intelligence Unit □ □□□□□ □□ □□□ □□□□□□ □□□□□.
D. □□□ □□□□ □□ □□ □□□□□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
According to the ACAMS CAMS Certification Study Guide, 6th Edition, one of the four pillars of an effective anti-money laundering compliance program is the training of appropriate employees on their responsibilities and the institution's policies and procedures. Training is essential to ensure that employees are aware of the risks of money laundering and terrorist financing, the applicable laws and regulations, the red flags and indicators of suspicious activity, and the reporting and record-keeping requirements. Without proper training, employees may not be able to perform their duties effectively and efficiently, and may expose the institution to legal, regulatory, reputational, and operational risks.
The other options are less serious deficiencies, but still need to be addressed and corrected. The compliance officer should have regular meetings with upper management to inform them of the

current money laundering trends and the status of the compliance program, but this is not as critical as providing training to the employees. The company's anti-money laundering manual should be updated to reflect any changes in the internal controls, policies, or procedures, but this is not as urgent as ensuring that the employees are familiar with the existing ones. The company should download the most recent regulation from the Financial Intelligence Unit web site, but this is not as important as complying with the existing ones.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 2, Section 2.1.4, page 39.
ACAMS CAMS Certification Video Training Course, Module 2, Lesson 2.1.4.

NEW QUESTION: 144
□□ □□□ SAR/STR□ □□□□□ □□□?
A. □□□□□□ □□□ □□ □□ □□ □ $9,950 USD□ □□□ □□□□□□.
B. □□□□□ □□□□□ □□□□□ □□ □□ □□□□□ □□ □□ □□□□□□ $25,000 USD□ □□□ □□□.
C. □□□ □□□□□ □□ □□ □□□ □□ □□ □□ □□ □□□□□.
D. □ □□ □□ □□ □□□□□□ □□ □□ □□□ □□□□□ □□ □□ □□□ □□ □ □□□.
Answer: A (LEAVE A REPLY)
Ref This transaction should result in a SAR/STR filing because it indicates possible structuring, which is a form of money laundering that involves breaking down large amounts of cash into smaller deposits to avoid detection or reporting requirements. Structuring is often done to conceal the source or destination of illicit funds, or to evade taxes, regulations, or sanctions. A small business owner who deposits checks just below the $10,000 USD threshold on a daily basis without providing a legitimate purpose raises a red flag for suspicious activity and should be reported to the relevant Financial Intelligence Unit.
Reference:
Suspicious Transaction Report (STR) / Suspicious Activity Report (SAR)
What Is a Suspicious Activity Report (SAR)? Triggers and Filing
How to decide if SAR filing is needed
erence: https://aml-cft.net/library/suspicious-transaction-report-str-suspicious-activity-report-sar/

NEW QUESTION: 145
□□□□□ □□□ □□ □□ □□ □□□ □□□ □ □□□□□□ □□□ □□□ □□□ □□□□□□? (2□□ □□□□□□.)
A. □□□ □□
B. □□□ □□
C. □3□□ □□□□□ □□□□□□ □□□□□ □□
D. □□□ □□ □□
E. □□□ □□□ □□ □□ □□
Answer: (SHOW ANSWER)

When implementing a risk-based approach related to casinos, the risks related to the customer as an individual are mainly based on the customer's profile, behaviour, source of funds, and geographic location. Among the options given, B and D are the most relevant factors that could indicate a higher risk of money laundering or terrorist financing.
Casual customers are those who do not have a regular or established relationship with the casino, and who may visit the casino only once or occasionally. They may not provide sufficient or reliable identification information, or may use false or stolen identities. They may also engage in suspicious transactions, such as large cash purchases of chips, minimal or no gaming activity, or frequent transfers of chips between customers. Casual customers pose a higher risk of money laundering or terrorist financing because they are harder to verify, monitor, and trace by the casino operators.
Customer from a high-risk country is a customer who resides in, or has links to, a country that is subject to sanctions, embargoes, or similar measures, or that is identified by credible sources as having significant levels of corruption, or as being a source, transit, or destination of illicit funds. Such customers pose a higher risk of money laundering or terrorist financing because they may be involved in, or connected to, criminal or terrorist activities, or may be using funds that are derived from or intended for such activities.

NEW QUESTION: 146
□□□ □□□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □ □□□□ □□ □□ □□□□□(Financial Action Task Force) □□ □ □□□□□.
B. □□□□□ □□ □□ □□□□□□ □□□□□ □□□□□.
C. □□□□ □□ □□□□ □ □□□ □□ □□
D. □□ □□□ □□ □□ □□ □□ □□□ □□ □ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The Egmont Group is a united body of 174 Financial Intelligence Units (FIUs) that uniquely support national and international efforts to counter terrorist financing and share financial information per global anti-money laundering and counter-financing of terrorism (AML/CFT) standards. Its primary objective is to enhance international cooperation in the investigation and prosecution of money laundering and financing of terrorism. The Egmont Group facilitates the exchange of expertise and financial intelligence among FIUs to combat money laundering, terrorist financing, and associated predicate offenses. While it does not conduct financial investigations itself, it plays a crucial role in improving stakeholders' understanding of ML/TF risks and informing policy considerations related to AML/CFT implementation and reforms12.

NEW QUESTION: 147
□□ □□□ □□□ □□□□ □□ □□□□□ □□ □□□□ □□□□ □□□□ □□□?
A. □□□□□□ □□ □□ □□□
B. □ □□□□ □□□□□□ □□□
C. □□□ □□ □□□□□□□ □□ □□□□ □

D. □□□ □□ □□ □□ □□ □□ □ □□□

Answer: (SHOW ANSWER)

According to the Anti-Money Laundering Specialist (the 6th edition) by ACAMS, the independent testing of an institution's anti-money laundering program should be conducted by a person who reports directly to the Board of Directors or a Board Committee. This ensures that the person conducting the testing has the necessary authority, independence, and objectivity to evaluate the program's adequacy and effectiveness, and to report any findings or recommendations to the senior management1. The person conducting the testing should also have the appropriate knowledge, skills, and experience in the anti-money laundering field, and should be familiar with the institution's products, services, customers, and risks2.

The other options are not necessarily suitable or qualified to perform the independent testing of an institution's anti-money laundering program. For example:

A certified specialist in the anti-money laundering field may have the relevant expertise and credentials, but may not have the required independence or reporting line to conduct the testing. For instance, if the certified specialist is an employee of the institution who is involved in the implementation or operation of the anti-money laundering program, then there may be a conflict of interest or a lack of objectivity in the testing process1.

A former anti-money laundering officer from a similar institution may have the relevant experience and background, but may not have the current knowledge or familiarity with the institution's anti-money laundering program, policies, procedures, or systems. Moreover, the former anti-money laundering officer may have a personal or professional relationship with the institution or its staff, which may compromise the independence or integrity of the testing process1.

A retired government regulator or federal law enforcement officer may have the relevant authority and credibility, but may not have the specific skills or qualifications to conduct the testing. For instance, the retired regulator or law enforcement officer may not be well-versed in the latest anti-money laundering standards, regulations, or best practices, or may not be able to apply them to the institution's unique risk profile, products, services, or customers1.

Reference:

Anti-Money Laundering Specialist (the 6th edition) by ACAMS

What Is An AML Compliance Program? | ComplyAdvantage

NEW QUESTION: 148

□□ □□ □□□ □□ □□□□□□ □□□ □□□ □□□ □ □□□□? (2□□□ □□□□□□.)

A. □□□ AML/CFT □ □□ □□ □□□ □□ □□□ □□□ □□ □□ □□ □□□ □□□□□□.

B. □□ □□ □□□ AFC(□□□□ □□) □ □□ □□ □□□, □□□ □ □□□ □□□□□□.

C. □□ □□□ □□ □□ □ □□□ □□.

D. □□ □□□ □□ □ □□.

Answer: (SHOW ANSWER)

Many jurisdictions lack robust sanctions frameworks, requiring international cooperation and education to improve compliance.

Option B (Correct): Educational initiatives such as AML/sanctions training and workshops help raise awareness and build capacity.
Option D (Correct): Bilateral cooperation allows knowledge-sharing and technical assistance between regulatory authorities.
Why Other Options Are Incorrect:
Option A (Incorrect): Trade restrictions may pressure non-compliant nations, but they do not directly improve sanctions awareness.
Option C (Incorrect): Enforcing fines without prior education or assistance is ineffective and may create diplomatic tensions.
Best Practices for Sanctions Awareness & Compliance:
Develop international AML/sanctions training programs for emerging markets.
Encourage diplomatic engagement to strengthen legal frameworks.
Leverage FATF's Mutual Evaluation process to assess progress.
Reference:
FATF Recommendation 6 (Sanctions & International Cooperation)
OFAC Guidance on Sanctions Compliance for Emerging Jurisdictions
Egmont Group Guidelines on Information Sharing & Capacity Building

NEW QUESTION: 149
□□ □ □□ □□□□□ □□□□ □□ □ □□ □□□□□ □□□□ □□ □□□ □□ □□□□□?
A. □□□ □□ □□□ □□□ □□□□□□□.
B. □□(□□) □□ □□ □□ □□□□□ □□□ □□□□□.
C. □□ □ □□ □□□□□ □□ □□ □□□□ □□□□□.
D. □□ □ □□ □□□ □□ □□□□□ □ □□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Conducting small cash transactions at multiple locations during the same day is the strongest example of avoiding reporting thresholds. This is a common technique used by money launderers to evade the attention of financial institutions and regulators, who are required to report cash transactions above a certain amount (usually $10,000) to the authorities. By splitting the large sum of money into smaller amounts and depositing them at different branches or ATMs, the money launderer can avoid triggering the reporting requirement and conceal the source and destination of the funds. This practice is also known as smurfing or structuring12.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 2, page 36
ACAMS CAMS Certification Video Training Course, Module 2, Lesson 2.2, Structuring and Smurfing
1, Smurfing Money Laundering: Mechanics, Detection, and Prevention
2, AML & eWallets - The Risks & How To Comply | ComplyAdvantage

NEW QUESTION: 150
□□□ □□ □□ □□(SUA)□ □□ □□□□□ □□ □□ □□?

A. □□ □□ □□ □□□ □□□□ □□□ □□□ SUA□ □□□□□ □□□.
B. SUA□ □□□□□ □□□ □□ □□ □□□□ □□□□□.
C. □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□ □□□□ □□□□□ □
D. SUA□ □□□ □□□ □ □□ □ □□□ □□□ □□□□ □□□ □□□□□.
Answer: A ([LEAVE A REPLY])
According to 18 U.S.C. § 1956, the money laundering statute, the property involved in a financial transaction must represent the proceeds of some form of unlawful activity, which is defined as a specified unlawful activity (SUA). SUAs include over 250 crimes in six categories, such as RICO predicate offenses, certain offenses against foreign nations, acts constituting a criminal enterprise under the Controlled Substances Act, and federal health care offenses. Therefore, in order to pursue a money laundering conviction, the government must prove that at least one SUA was committed and that the property involved in the transaction was derived from that SUA.
Reference:
18 U.S. Code § 1956 - Laundering of monetary instruments, (a)(1) and ©(7).
957. Money Laundering-18 U.S.C. §§ 1956 & 1957, first paragraph.
Specified Unlawful Activities (SUA), first paragraph.

NEW QUESTION: 151
□□□ □□ □□ □□ □□□□□ □□ □□□□ □□□□□ □□ □□□ □□□ □□□?
A. □□□□□ □□□□□ □□□ 6□□□□ □□□□ □□□□□□□ □□□.
B. □□□□□ □□□ □□□ □□ □□ □ □□□□ □□□ □□□ □□□.
C. □□□□□ □□□□□ □□□ □□ □□ □□□ □□□ □□□.
D. □□□□□ □□□ □□ □□□□□□ □□□.
Answer: D ([LEAVE A REPLY])
According to the Anti-Money Laundering Specialist (the 6th edition) by ACAMS, an institution's anti-money laundering program should be reassessed at least annually to ensure that it is current, effective, and compliant with the applicable laws and regulations. The reassessment should include a review of the institution's risk assessment, policies and procedures, internal controls, training, and independent testing. The reassessment should also consider any changes in the institution's products, services, customers, geographic locations, or business environment that may affect its exposure to money laundering and terrorist financing risks1.
The other options are not consistent with the best practices of maintaining an up-to-date anti-money laundering program. For example:
The program should be evaluated and updated at least every six months by the Board of Directors. While the Board of Directors has the ultimate responsibility for overseeing the institution's anti-money laundering program, it is not required to evaluate and update the program every six months. This may be too frequent and impractical, especially for large and complex institutions. The Board of Directors should, however, approve the program and any significant changes, and ensure that senior management implements and enforces the program effectively1.
The program should be reviewed by a federal law enforcement officer for gaps in controls. While federal law enforcement agencies may conduct investigations or examinations of the institution's

anti-money laundering program, they are not responsible for reviewing the program for gaps in controls. This is the role of the institution's internal audit function or an external independent party, who should conduct periodic testing of the program's adequacy and effectiveness1.
The program should be sent to the institution's government regulator on a periodic basis. While the institution's government regulator may request or review the institution's anti-money laundering program as part of its supervisory or enforcement activities, the institution is not obligated to send the program to the regulator on a periodic basis. The institution should, however, report any suspicious or unusual transactions or activities to the relevant authorities, such as the Financial Crimes Enforcement Network (FinCEN) or the Office of Foreign Assets Control (OFAC)1.
Reference:
Anti-Money Laundering Specialist (the 6th edition) by ACAMS

NEW QUESTION: 152
□□ □□□□□ □□ □□□□ □□□□ □□□□ □□ □□□□ □□□□□ □□ □□□□ □□□□□□. □□□□ □□□□□ □□ □□□□ □□ □□□□□ □□ □□□□ □□□□□ □□ □□ □ □□ □□□□ □□□□ □□ □□ □□□□ □□ □□□□ □□□□□□. □3□□ □□□□ □□□□ □ □□□□ □□□□□□. □□□□ □□ □□□□, □□□□ □□ □□ □□, □□ □□ □□□□ □□□□□□. □□ □ □□ □□□□ □□ □□ □□ □□ Banks Paper□ □□ □□ □□□□□ □□□□□ □□ □□ □□□□ □□□□□ □□ □□□□ □□ □□□□□ □□□□ □□□□□□?
1. □□□□□□ □□□□□ □□ □□ □ □□□□□□ □□ □□□□□□.
2. □□□□ □□□□ □□□□ □□□□ □□□□□□ □□□□□□□.
3. □□□□ □□□□ □□□□□□□□□ □□ □□ □□□□ □□ □□□□ □□□□□□□.
4. □□□□□□ □□□□ □□□□ □□□□□ □□ □□ □□□□ □□ □□□□ □□□□□ □□□□□□.
A. 1□ 2□
B. 1□ 4□
C. 2□ 3□
D. 3□ 4□
Answer: C (LEAVE A REPLY)
The Basel Committee on Banking Supervision's Customer Due Diligence for Banks Paper recommends that banks should verify the bank has a physical presence in the country where it is incorporated and confirm the bank is subject to regulatory supervision with adequate anti-money laundering laws before opening a correspondent account. These steps are intended to prevent

the establishment of relationships with shell banks, which are banks that have no physical presence in any country and are not affiliated with a regulated financial group. Shell banks pose a high risk of money laundering and terrorist financing, as they can be used to hide the identity and source of funds, evade regulatory oversight, and facilitate illicit transactions. Therefore, banks should conduct enhanced due diligence on correspondent banks that operate in offshore jurisdictions, where the regulatory standards and transparency may be lower or insufficient.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 4, Section 4.3.1, p. 1091 ACAMS CAMS Certification Exam Outline, 6th Edition, Domain 2, Task 2.2, p. 52 Basel Committee on Banking Supervision, Customer Due Diligence for Banks, October 2001, p. 13-143

NEW QUESTION: 153
□□□ □□□ □□ □□□ □□ □□ □□ □□□□□. □□ □□□ □□□ □□□□□ □□□ □ □□□□ 15,000 USD□□ □□ 30,000 USD□□ □□ □□□□ □□□ □□□□. □□□□ □□ □□ □□□ □□□ □□□□.
□□□□ □□□ 90%□ □□□ □□□□ □□□□. □□ □□ □□
□□□□ □□□□□ □□ □□□□□□?
A. □□□ □□□□ 90%□ □□□ □□□□ □□□□ □□□□ □□□□.
B. □□□ □□ □□ □□ □□□□□.
C. □□□ □□ □□□□ □□□□□ □□□ □□ □□□ □□□□□ □□□□.
D. □□□ □□ □□ □□□□ □□□ □□ □□ 15,000 USD□□ 30,000 USD□ □□□□□□.
Answer: A (LEAVE A REPLY)
The customer's business activity as a domestic carpet cleaning company is not inherently suspicious, as it aligns with their registered business. However, the significant weekly transactions from an international reputable antique auction house raise red flags.
The sudden increase in the customer's initial international receipt from $15,000 USD to an average of $30,000 USD per transaction per week is also noteworthy. Such a substantial change warrants further scrutiny.
The fact that 90% of the incoming deposits are matched by cash outgoings to non-related individuals could indicate layering or structuring activities associated with money laundering.
Overall, the combination of large international transactions, increased receipts, and cash outflows to unrelated parties from an antique auction house is the most concerning aspect.
Reference:
Anti-Money Laundering Specialist (the 6th edition) resources.
ACAMS AML Glossary (definitions of terms related to AML).1
ACAMS AML Foundations Certificate (overview of AML concepts and responsibilities).2
ComplyAdvantage: 6th Money Laundering Directive (6AMLD) (details on AML regulations and penalties).3

NEW QUESTION: 154

□□□□□□ □□ □□□(SAR)□ □□□ □ □□□□□ □□□ □□ □□□□□ □□□□□ □□ □□ □
□□□□?

A. □□□ □□ □□ □□□ SAR□ □□□ □□ □□ □□

B. □□ □□ □□ □□□ SAR □□□ □□ □□□ □□

C. □□□ □□ □□ □□□ SAR□ □□ □□ □□□

D. □□ □□ □□ □□□ □□ SAR□ □□

Answer: (SHOW ANSWER)

The board of directors or designated specialized committee should be provided with statistical data regarding SARs filed during the reported period, such as the number, type, and amount of SARs, as well as any trends or patterns identified. This would enable them to oversee the effectiveness of the anti-money laundering program and ensure compliance with regulatory requirements. Providing too much detail, such as names of customers or copies of SARs, could compromise the confidentiality of the SARs and expose the institution to legal risks.

Reference:

ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 5, page 153, section "Reporting to the Board of Directors or Designated Specialized Committee".

ACAMS CAMS Certification Video Training Course, Module 5, Lesson 5.4, "Reporting to the Board of Directors or Designated Specialized Committee".

NEW QUESTION: 155

□□ □□□ □□□□□ □□□□□ □□□□ □□□□□ □□ □□□ □□ □□ □□□ □□□□□□ □□
□ □□□□□□□□. □□ □ □□□□□□□ □□□□□ □□□□□□ □□ □□□□□ □□□□□ □□ □
□ □ □□ □□□□□?

A. □□□□□□ □□ □ □□ □□□ □□□ □□□ □□□□□□.

B. □□□□□ □□ □□ □□□□□□ □□□□□□.

C. □□□ □□ □□ □□□ □□□□□□ □□□ □□□ □□□ □□□□□□.

D. □□□□□□ □□ □□□ □□ □□□□□ □□□□□ □□ □□□ □□□□□□.

Answer: A (LEAVE A REPLY)

The anti-money laundering specialist should secure all the documents related to the suspicious activity and the decision to report before submitting the suspicious transaction report (STR). This is to ensure that the evidence is preserved, the confidentiality is maintained, and the audit trail is documented. The documents may include the customer identification, transaction records, account statements, monitoring alerts, investigation reports, and any other relevant information12. Checking with other financial institutions, adding information to the customer's file, or contacting the customer are not appropriate actions to take before submitting the STR. These actions may compromise the confidentiality of the report, alert the customer of the suspicion, or interfere with the investigation by the competent authorities12.

NEW QUESTION: 156

□□□□□ □□ □ □□ EU □□□ □□ □□□ □□□□□□?

A. IT□ □□ □□□ □□□ □□ □□□□□ □□□□□□□.

B. □□□□□ □□□ □□□ □□□□□□□.
C. □□ □□□ □□ □□□ □□ □□□ □□□□□□□.
D. □□ □□ □□□ □□ □□□ □□□□□□□.
Answer: (SHOW ANSWER)
IT expanded the definition of criminal activity to all serious crimes. The first EU Directive on Money Laundering, adopted in 1990, was the first major international agreement to combat money laundering. It expanded the definition of criminal activity to all serious crimes and established drug trafficking as a predicate offense of money laundering. The Directive also extended the scope of money laundering beyond drug-related crimes, making it applicable to all serious crimes. This was a major step forward in the fight against money laundering, as it made it easier for law enforcement to investigate and prosecute money laundering cases.

NEW QUESTION: 157
□□ □□ □ SAR/STR □□ □□□ □□ FATF □□□ □□ □□□□□ □□ □□?
A. FI□ STR□ □□□ □□□□□□ 5□ □□ SAR/STR □ □□ □□□ □□□ □□□□□ □□□.
B. FI□ □□ □□□ □□□□□ □□□ □□ □□□ □ □□□□□.
C. □□ □□(FI)□ AML □□□□□ □□□□□ □□□ □□□□□ □□□□□ □□□ □□ □□□ □□□ □ □□□.
D. FI□ SAR/STR □□ □ □□ □□□ □□□□□ □□ □□ □□□ □□□ □□□ □□□.
Answer: C (LEAVE A REPLY)
According to the FATF Guidance on Private Sector Information Sharing, FIs should establish sufficient safeguards concerning the confidentiality of information shared for AML purposes, both within the same financial group and between FIs not belonging to the same group. These safeguards include ensuring that the information is shared only with authorized personnel who have a need to know, that the information is used only for the intended AML purpose, and that the information is protected from unauthorized access, disclosure, or misuse. FIs should also comply with the applicable legal and regulatory requirements on data protection and privacy, and respect the rights and interests of the customers whose information is shared1.
Reference:
1: FATF Guidance on Private Sector Information Sharing1

NEW QUESTION: 158
□□ □□ □□ □□□□□ □□□□□□ □□ □□□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□ □□□□□□. □ □□□□□ □□ □ □□□ □□ □□□□□ □□□ □□□□□□?
A. □□□□□□ □□ □□□ □□□ □□□□□ □□□□□ □□ □□□□□□.
B. □□□□□□ □□□□□□ □□□□□□ □□□□□ □□.
C. □□□□□ □□□ □ □□□□□ □□□ □□.
D. □□□□□ □□□□□ □ □□□□□ □□□ □□□.
Answer: D (LEAVE A REPLY)
According to the BSA/AML Manual1, a financial institution's board of directors and senior management are ultimately responsible for ensuring that the institution has a comprehensive and

effective BSA/AML compliance program and oversight framework. This includes ensuring that the institution timely identifies, reports, and responds to suspicious activity involving its products, services, customers, or employees. Therefore, when an anti-money laundering specialist is concerned that several suspicious transaction reports will discuss potential illegal activity of bank employees, the immediate concern for the institution is to ensure no delay in informing the board of directors and senior management of the situation, as well as the actions taken or planned to address the risks and mitigate the potential harm. The board and senior management should be kept informed of the status and outcome of any internal or external investigations, as well as any regulatory or law enforcement inquiries or actions, related to the suspicious activity involving bank employees.

Reference:

BSA/AML Manual1

Suspicious Activity Reporting - Overview2

Suspicious Activity Report (SAR) Basics3

What's Suspicious? Here's How Banks Apply the Smell Test4

NEW QUESTION: 159

□□□ □□ □ □ □□ □□□ □□□□ □□□□□. □□□ □□□□□(FIU)□ □□□□ □□□ □ □□□ □□□□ □□□.

A. □□□ □□ □□□ □□□□ □□□□□ □□ □□□(SAR)□ □□□□□.

B. □□ □□□ □□□□ □□□□ □□□ □□□□□.

C. □□□□ □□□□ □□□□ □□ □□□ □□□□□.

D. □□□□□□ □□ □□□ □□□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

Banks must comply with legal subpoenas while ensuring AML compliance.

Option B (Correct): The bank should review client transactions and respond fully to law enforcement.

Option A (Incorrect): Filing a SAR simply because of a subpoena is not required unless suspicious activity is identified.

Option C (Incorrect): Tipping off the client about the subpoena is illegal under AML laws.

Option D (Incorrect): Risk scores should be reviewed but not automatically adjusted solely based on a subpoena.

NEW QUESTION: 160

□□ □□□ □□□ □□□ □□□ □□□□□□. □□□ □□ □□□ □□□□ □□□ □ □□□ □□ □□□ □□□□ □□□.

A. □□ □□□ □□□□ □□□□□.

B. □ □□□ □□ □□□ □□□□.

C. 30□ □□ □□□ □□□ □□□□□□□.

D. □□□ □□□ □□□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

According to the CAMS Certification Package - 6th Edition1, one of the essential components of customer due diligence is verifying the identity of the customer using reliable and independent sources. This verification process should be done before or during the establishment of the business relationship, and should not be delayed unless there is a low risk of money laundering or terrorist financing, and the delay is necessary to avoid interrupting the normal course of business. Therefore, after customers have provided acceptable identification, the financial institution should next confirm the validity of the customer information, as option A suggests. Option B is not necessary, as an electronic picture of each customer is not a mandatory requirement for customer verification, and may not be feasible or effective in some cases. Option C is not the next step, as closely monitoring the account for 30 days is part of the ongoing due diligence process, which should be performed after the customer verification is completed and the account is established. Option D is not advisable, as establishing the account based on the information provided without verifying its validity may expose the financial institution to money laundering and terrorist financing risks, and may violate the KYC and AML regulations.
Reference:
1: CAMS Certification Package - 6th Edition | ACAMS, Chapter 3: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), pages 69-70.

NEW QUESTION: 161
□□□ □□□□□ □□□□□□□ □□ □□□ □□□□□ □□□□□□ □□ □□□□□□ □□□□ □□ □ □□□ □ □□ □□ □□□ □□□□□□?
A. □□ □□□□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□□□□.
B. □□ □□□□□□ □□□ □□ □ □□□ □□□ □□□□ □□ □□□□□□□.
C. □□ □□□ □□□ □□ □□ □□ □□□ □□□□ □□ □□□□□□ □□ □□□ □□□ □□ □□□□□□□.
D. □□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Money launderers prefer large-denomination bills because they facilitate bulk cash smuggling and placement.
Option A (Correct): Increased demand for large-denomination banknotes is a known money laundering red flag.
Option B (Incorrect): Increased digital service adoption is normal banking behavior.
Option C (Incorrect): Faster settlement times may reflect technology upgrades, not financial crime.
Option D (Incorrect): Maintaining a log of monetary instruments is a compliance best practice, not a red flag.

NEW QUESTION: 162
Financial Action Task Force Regional-Style Bodies□ □□□ □□□□□?
A. □□ AML □□ □ □□ □□

B. □□□ □□ □□□□□□□ □□ □□□ □□ □□□□□ □□□□□ □□□ □□ □□ □□ □□ □
□ □□
C. □□ □□□ □□ □□□ AML □□□□□ □□
D. □□□ □□□ AML □□□ □□□ □□□ □□□□□ □□ □□ □□
Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 163
□□ □□□(USA PATRIOT Act)□ □□ □ □□□ □□□□□□?
A. □□ □□ □□ □ □□ □□ □□□ □□, □□ □ □□□□□ □□ □□□ □□□ □□□□□□.
B. □□□ □□ □□□ □□ □□ □ □□ □□□ □□□□□ □□.
C. □□ □□□ □□ □ □□□ □□ □□ □□□ □□□□□□.
D. □□□ □□□ □□ □□ □□(FI) □ □□ □□ □□□ □□ □□□ □□□□□□.
Answer: D ([LEAVE A REPLY](#))
The USA PATRIOT Act, enacted in 2001, is a comprehensive legislation that aims to enhance the US government's ability to combat terrorism, money laundering, and other criminal activities. One of the aspects of the Act that has extraterritorial reach is the requirement for US financial institutions (FIs) to apply certain due diligence and reporting obligations to their correspondent accounts and private banking accounts for foreign FIs and non-US persons, respectively12. These obligations are intended to prevent foreign FIs and individuals from using the US financial system to facilitate money laundering, terrorist financing, or other illicit activities. The Act also authorizes the Secretary of the Treasury to impose special measures, such as recordkeeping, reporting, or prohibitions, on certain foreign jurisdictions, FIs, or transactions that are found to be of primary money laundering concern34. These special measures can have significant impact on the access and operations of foreign FIs and persons in the US financial market.
Reference:
1: USA PATRIOT Act, Title III, Subtitle A, Section 3121
2: 31 CFR 1010.610 - Due diligence programs for correspondent accounts for foreign financial institutions2
3: USA PATRIOT Act, Title III, Subtitle A, Section 3113
4: 31 CFR 1010.651 - Imposition of special measure against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern4

NEW QUESTION: 164
□□ □□□ □□□ □□□ □□ □□ □□ □□□ □□□ □□□□. (2□ □□)
A. □3□□ □□ □□ □□□ □□ □□ □□.
B. □□□ □□□ □□ □□ □□ □□ □□□□□ □□□ □□□□□□.
C. □□ □□ □□□□□□□ □□ □□□ □□□□□□ □□□□□□.
D. □□□ □□□ □□□□□ □□□□□ □□ □□□ □□ □□□□□.
E. □ □ □□□ □□□ □□□ □□ □□ □□□ □□□ ID□ □□□□□□.
Answer: B,E ([LEAVE A REPLY](#))

These two options are indicative of money laundering red flags associated with money service businesses, as they may suggest attempts to avoid reporting requirements, conceal the source or destination of funds, or use false or stolen identities. Money service businesses are vulnerable to money laundering due to the high volume and anonymity of transactions, the ease of cross-border transfers, and the lack of effective regulation and supervision in some jurisdictions12. Therefore, they should implement robust anti-money laundering policies and procedures, and monitor and report any suspicious activity.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 3, page 631
ACAMS CAMS Certification Video Training Course, Module 3, Lesson 42

NEW QUESTION: 165
□□□ □□□ □□ □□□ □□ □□□□ □□ □□□(MLRO)□ □□□□ AML □□ □□□□ □ □□□ □□□□□ □□□ □□□□□.
AML □□□□ □□□□ □□□□ □ □□ □□□ □□ □□□ □□□□□? (2□□ □□□□□.)
A. □□□ □□, □□, □□□ □ □□□ □□□ □□□□ □□□□ □□□□ □□.
B. □□□□□ □□□ □ □□□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□□□□□ □□.
C. □□□□□ □□□ □□□ □□ □□□ □□, □□, □□□□ □□ □□ □ □□□ □□□ □□ □ □□ □□□□ □□□□ □□ □ □□□ □□□ □□□□ □□.
D. □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□□ □□□□ □□ □ □□□ □□□ □ □□□ □□□□ □□□□ □□□ □ □□□ □□□□□.
Answer: A,D (LEAVE A REPLY)
An effective AML transaction monitoring system must align with the bank's operational complexity, risk exposure, and analytical capabilities.
Option A (Correct): The system must be tailored to the bank's specific risk profile to ensure effectiveness.
Option D (Correct): A strong AML system should support trend analysis to identify long-term suspicious behaviors.
Why Other Options Are Incorrect:
Option B (Incorrect): While vendor controls are important, they do not determine system suitability.
Option C (Incorrect): User access settings should be based on the bank's internal risk framework, not industry standards alone.
Best Practices for Implementing an AML Monitoring System:
Ensure scalability to adapt to evolving financial crime risks.
Leverage AI and machine learning to enhance detection accuracy.
Integrate real-time screening and transaction trend analysis.
Reference:
FATF Recommendation 10 (Customer Due Diligence & Monitoring)
Wolfsberg Group Guidance on AML Technology Implementation

Basel Committee's Guidelines on Transaction Monitoring System Effectiveness

NEW QUESTION: 166

□□ □□ □□□ □□, □□ □ □□□□□ □□□ □□ □□ □□ □□□□□ □□ □□□ □□□□□ □□ □□ □□□□□ □□□?

A. □□□□ □□

B. □□□□□□□ □□

C. □□□□ □□□□□□

D. □□ □□□

Answer: (SHOW ANSWER)

it describes the organization that a national Financial Intelligence Unit (FIU) should consider becoming a member of, which is the Egmont Group. The Egmont Group is an international network of FIUs that was established in 1995 to facilitate the exchange of financial intelligence and information among its members, and to promote cooperation and coordination in the fight against money laundering and terrorist financing. The Egmont Group currently has 166 member FIUs from different jurisdictions, and provides them with various benefits, such as access to secure communication channels, best practices, training, and technical assistance. The Egmont Group also works closely with other international organizations, such as the Financial Action Task Force (FATF), the United Nations, and the World Bank, to enhance the global anti-money laundering and counter-terrorist financing (AML/CTF) framework.

The other options are not necessarily organizations that a national FIU should consider becoming a member of, although they may have some relevance or influence on the AML/CTF field. Option B describes the Wolfsberg Group, which is an association of 13 global banks that was formed in 2000 to develop standards and guidance for the financial industry on AML/CTF and other financial crime issues. The Wolfsberg Group is not an organization for FIUs, but rather for financial institutions. Option C describes the Financial Action Task Force (FATF), which is an inter-governmental body that was established in 1989 to set the international standards and recommendations for AML/CTF and to monitor the compliance and effectiveness of its members and other jurisdictions. The FATF is not an organization for FIUs, but rather for governments and policy-makers. Option D describes the Basel Committee, which is a forum of central bank governors and heads of banking supervision authorities from 28 jurisdictions that was established in 1974 to enhance the quality and consistency of banking supervision and regulation. The Basel Committee is not an organization for FIUs, but rather for banking regulators and supervisors.

Reference:

ACAMS CAMS Certification Video Training Course - 6th Edition1

Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)2 ACAMS CAMS Study Guide - 6th Edition, Chapter 5, pages 108-109

: https://www.acams.org/wp-content/uploads/2019/09/ACAMS-CAMS-Study-Guide-6th-Edition-Chapter-5.pdf

NEW QUESTION: 167

□□□□□ □□ □□□□□ □□ □□□□ □□ □□□□ □□ □□ □□□□ □□□□□ □□ □□□□ □□□□ □ □□□□ □□ □□ □□□□ □□ □□□□ □□□□□□.

2001□ □□ □□□□□□ □□, □□ □□ □□□□ □□ □□□□□□ □□□□ □□□□□ □□ □□□□ □ □ □□ □□□□□□□ □□□□ □□□□□ □□□□ □□□□.

2001□ □□ □□□□□ □□ □□□□ □□ □□□□ □□ □□□□ □□□□□□ □□□□□□? (3□□ □□ □□□.)

A. □□ □□□□ □□□□ □□□□□□□□□.

B. □□ □□□□ □□□□□□ □□□□ □□(PEP)□ □□ □□ □□□□ □□□□□□ □□□□□ □□ □□ □□ □□□□.

C. □□ □□□□ □□□□□□ □□□□□ □□ □□ □□□□.

D. □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□□□.

E. □□ □□□□ □ □□□□ □□ □□ □□□□ □□□□□□ □□□□□ □□ □□□□□ □□□□□.

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

The USA PATRIOT Act Section 313 & 319(b) places strict requirements on foreign correspondent banking relationships to prevent money laundering.

Option A (Correct): The foreign bank must disclose its ownership structure to identify ultimate beneficial owners (UBOs).

Option C (Correct): The foreign bank must certify that it maintains a physical presence in a regulated jurisdiction.

Option E (Correct): The foreign bank must not allow shell banks to use its U.S. correspondent accounts.

Why Other Options Are Incorrect:

Option B (Incorrect): The certification does not specifically exclude PEPs, but PEPs require enhanced due diligence (EDD).

Option D (Incorrect): The foreign bank may operate in multiple jurisdictions, but it must be regulated where it has a presence.

Key Compliance Measures for Correspondent Banking:

Conduct EDD on foreign bank relationships.

Ensure correspondent banks do not facilitate shell banks.

Monitor transactions for money laundering and terrorist financing risks.

Reference:

USA PATRIOT Act Section 313 & 319(b) (Foreign Correspondent Banking Rules) FATF Recommendation 13 (Correspondent Banking Due Diligence) Wolfsberg Group Guidance on Correspondent Banking Risk Management

NEW QUESTION: 168

□□ □ □□□ □□ □ □□□ □□□□ □□ □□ □□□□□(Financial Action Task Force) □□ □ □□□ □□ □□□□□?

A. □□□ □ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □ □□□ □□ □□□□ □□

B. □□ □□□ □□ □□ □□□ □□□ □□ □□□ □□ □□□ □□

C. □□□ □□ □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□

D. □□ □□ □□□□□(Financial Action Task Force) 40 □□ □□□ □□□ □□ "□□□□□" □□ □□ "□□□□□" □□□ □□□□ □□□ □□

Answer: (SHOW ANSWER)

One of the criteria that the Financial Action Task Force (FATF) uses to define non-cooperative countries and territories (NCCTs) is the lack of adequate rules for the licensing and creation of financial institutions, especially those with no or minimal presence, and the lack of effective systems for checking the backgrounds of managers and beneficial owners of such institutions. This criterion aims to prevent the establishment and operation of shell banks or other entities that can be used for money laundering or terrorist financing purposes. The FATF requires that countries and territories should have laws and regulations that ensure that financial institutions are subject to adequate licensing or registration procedures, that the authorities have the power to deny or revoke licenses or registrations, and that the authorities have access to information on the identity, reputation, and financial soundness of the managers and beneficial owners of financial institutions.

Reference:

About the Non-Cooperative Countries and Territories NCCT Initiative, Section "The review and listing process": "The FATF established at that time four regional review groups (Americas, Asia/Pacific, Europe, Africa/Middle East) consisting of representatives from the FATF member governments that served as the main points of contact with the reviewed country or territory. ... The review groups gathered relevant laws, regulations and other relevant information, analysed this information against the 25 NCCT criteria, and drafted a report that was sent to the jurisdictions for comment." Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review, Annex 1: "List of Criteria for Defining Non-Cooperative Countries or Territories", Criterion 1: "Licensing and creation of financial institutions, in particular those with no physical presence, and the ability to obtain information on the beneficial ownership and control of such institutions." FATF (Financial Action Task Force) Countries 2024 - World Population Review, Section "Blacklisted Countries": "These are countries which were previously placed on the grey list and advised by the FATF to adopt the recommended financial security procedures, but have either failed or refused to do so. Blacklisted countries may be labeled as Non-Cooperative Countries or Territories (NCCTs)."

NEW QUESTION: 169
□ □□□□. □□□ □□ □□ □□, □□ □□ □□ □□□□ □□□□ KYC □□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□□□□.
A. □□□□, □□, □□, □□
B. □□, □□, □□, □□
C. □□, □□, □□, □□
D. □□, □□, □□, □□
Answer: (SHOW ANSWER)
The Basel Committee on Banking Supervision identified four risks to banking institutions as a result of an inadequate KYC program: legal, reputational, operational, and concentration. Legal risks include the potential for fines or sanctions for non-compliance with applicable laws and regulations. Reputational risks include the loss of customer confidence due to the institution's involvement in illicit activities. Operational risks include the potential for fraudulent or suspicious activity to go undetected. Finally, concentration risks involve the potential for a single customer or group of related customers to dominate the institution's operations.

NEW QUESTION: 170
□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□ □ □□□ □□ □□ □□□□ □□□ □□ □ □ □□ □□□ □□□□□.
□□ □□□ □□□□ □□ □□□ □□ □□ □□ □□□□□ □□□ □ □□□□?
A. □□ □□□ □ □ □□ □□□ □□□ □□ □□□ □□□□ □□□□ □□□□.
B. □□ □□□ □□ □□ □□□□□ □□ □□ □□ □□□□ □□□ □□□□ □□□□□.
C. □□ □□□ □□ □□□ □□ □□□ □□□□□ □□□ □□□ □□□□ □□□□□.
D. □□□□□ □□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□ □ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
having an outdated and incomplete risk assessment could expose the financial institution to significant money laundering and terrorist financing risks that are not identified, measured, or mitigated. The risk assessment is a key component of an effective anti-money laundering program, and it should be updated regularly to reflect the changes in the business environment, customer profile, product offerings, delivery channels, and regulatory requirements12. A risk assessment that is several years old and does not cover all current products and services could fail to capture the emerging threats and vulnerabilities that the financial institution faces, and could result in inadequate or inappropriate controls, policies, and procedures. This could lead to the highest potential for unmitigated risk, as the financial institution could be exploited by money launderers and terrorist financiers, and face regulatory sanctions, reputational damage, and financial losses.
Reference:
Anti-Money Laundering (AML) Risk Assessment | ACAMS1
Risk assess your business for money laundering supervision - GOV.UK2

NEW QUESTION: 171

□□ □ FATF□ □□ □□(FI)□ □□□ □□□ □□ □ □□(DNFBP)□ □□□ □□□□□ □□ □ □□(PEP)□□ □□ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□□?

A. PEP □□□ □□ □□ □□□ □□□□□□□□ □□□□□.

B. □ □□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□□ PEP □□□ □□ □ □ □□□□ □□□□ □□□□.

C. □□ □□ □□ □□ □□□ □□ □□ □□ □□□ □□□ □□□□□.

D. PEP□ □□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□□□, □□□ □□□ □□□ □□ □□□ □□□.

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

PEPs pose higher risks for corruption and money laundering, requiring enhanced due diligence (EDD).

Option D (Correct): Understanding a PEP's source of wealth and funds ensures legitimacy of transactions.

Option A (Incorrect): Commercial databases help identify PEPs but do not mitigate risk alone.

Option B (Incorrect): Lowering monitoring thresholds, not raising them, helps detect suspicious activity.

Option C (Incorrect): Regulatory approval is not required, but internal risk assessments are.

NEW QUESTION: 172

□ □□ □□□ □ □□□ □□□, □□□□□ 2□□ □□ □□ □□ □□□□□ □□□ □□, □, □□, □□□□ □□ □□□ □□□□□□.

□ □□□□ □□ □□□□□□ □□ □□□ □□ □□□ □□□□□ □□□ □□ □□ □ □□ □ □□ □□ □□□□□□ □□ □□ □□□ □□ □□□□□ □□□□ □ □□□□ □□□ □□ □ □ □□□□ □□□ □□□□□.

□ □□□ □□□ □□□□□?

A. □ □□□

B. □□

C. □□ □□

D. □□-□□ □□□□

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

Wash trading is a form of market manipulation where two parties coordinate to create artificial trading activity, often for money laundering, tax fraud, or price manipulation.

Why Option C (Wash Trading) is Correct:

No real market risk is taken-transactions are simply cycled between the same parties.

Creates an illusion of liquidity or inflates asset prices artificially.

Common in commodities, stocks, cryptocurrency, and futures markets.

Red flag for money laundering: Criminals may use wash trading to layer illicit funds through financial markets.

Why Other Options Are Incorrect:
Option A (Short Position): A short position involves selling an asset one does not own and repurchasing it later at a lower price-this does not describe the described scheme.
Option B (Reverse Flip): A reverse flip is a real estate money laundering typology, not applicable here.
Option D (Bid-Ask Spread): This refers to the difference between the highest price a buyer is willing to pay and the lowest price a seller will accept, but it does not involve fraudulent trading.
AML Risks in Wash Trading:
Can be used to move illicit funds through financial markets.
Artificially increases trading volume and market price manipulation.
Frequently flagged in AML transaction monitoring systems.
Best Practices for Detecting Wash Trading:
Monitor repetitive trading between related entities.
Look for circular transactions with no economic justification.
Use AI-based transaction monitoring to detect high-frequency wash trades.
Reference:
FATF Report on Money Laundering in Capital Markets
SEC & CFTC Enforcement on Wash Trading Cases
Wolfsberg Group Market Manipulation Risk Guidelines

NEW QUESTION: 173
□□□ □□□ □□ □□ □□□ □□ □□ □□□□□□ □□□□□ □□□-□□□ □□ □□ □□□ □□□□□. □□□ □□□ 2,550□ □□□ □□□□ 3□ □□ 500□ □□□ □□ □□□□ □□ □□□. □ □ □□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□□. □□□□□□□ □□ □ □□ □□ □□□ □□□□. □□ □□ □ □ □ □□□ □□□ □□□ □□□□□□□.
□□□ □□ □□□□ □□□ □□□□ □□□□ □□ □ □□ □□ □□□ □□□□□? (2□□ □ □□□□.)
A. □ □□ □□□ $2,550□□□□.
B. □□ □□□□□ □□□□ □□ □□□ □□□
C. □□□□ □□□ □□ □□□□□
D. □□□ □□□ □□ □□□ □□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
A corporate account opened on behalf of several beneficial owners is a red flag because it may indicate an attempt to conceal the identity or source of funds of the ultimate beneficiaries1. The customer's stated investment goal of long-term investment is not reflective of the account activity, which involves frequent and large transfers, currency exchanges, and account depletion within a short period of time. This discrepancy may suggest that the customer is using the account for money laundering or other illicit purposes2.

NEW QUESTION: 174

□□□ □□□□□□ □□□□□ □□□ □□□ □□□□□□. □□ □ □□ □□ □□ □□□□□. □□□ □ □□ □□ □□ □□□ □□□□□ □□ □□□ □□□□□ □□.
□□ □□ □□□ □□□□□ □□□ □□ □□□□□ □□□□□□. □□□ □□□ □□ □□□?
A. □□□□□ □□□□□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□.
B. □□□ □□□□□ □□□□□, □□□ □□ □□ □□ □□□ □□ □□ □ □□□□□□ □□□ □□ □□□□□ □□□.
C. □□□ □□□□□□□ □□□□□ □□□□□ □□□□□ □□ □□□□□□ □□ □□□□□ □□□□□ □ □□.
D. □□□ □□ □□□ □□□□□ □□ □□□ □□□□□ □□□.
Answer: (SHOW ANSWER)
A large cash deposit is a potential indicator of money laundering, especially if it is inconsistent with the customer's profile or behavior. Therefore, the bank should ask the customer about the source and purpose of the funds, and verify the information if possible. In this case, the customer claims to have sold a used car and received cash, which may be a reasonable explanation. However, the bank should not rely solely on the customer's statement, but should also monitor the account for any further cash transactions or suspicious activity that may indicate money laundering. For example, the bank should check if the customer withdraws the cash soon after the deposit, transfers the funds to other accounts or jurisdictions, or engages in structuring or smurfing to avoid reporting thresholds.
The bank should not do nothing, as this may expose the bank to regulatory or reputational risks, or facilitate money laundering. The bank should also not file a Suspicious Transaction Report (STR) unless there are other grounds to suspect money laundering, as this may be premature or unnecessary. The bank should not close the account before another issues arise, as this may be disproportionate or discriminatory, and may also alert the customer to the bank's suspicion.
Reference:
[ACAMS Study Guide for the CAMS Certification Examination, 6th Edition], Chapter 4: Conducting or Supporting the Investigation Process, pp. 103-104, 107-108.
Customer Identification Program - Overview, Federal Financial Institutions Examination Council, April 2018, pp. 1-2, 4-5.
Suspicious Activity Reporting - Overview, Federal Financial Institutions Examination Council, April 2018, pp. 1-2, 4-5.
18 AML Analyst Interview Questions (With Example Answers), ResumeCat, accessed on February 9, 2024.

NEW QUESTION: 175
□□□□□□ □□□□□□□ □□□□□ 2004□□□ □□ □□□ □□ □□□□□□ □□□ □□□ □□ □□□ □□□□□□. □□ □ □□ □□ □□□□□□ □□□?
1. 2004□ □□ □□ □□□ □□ □□□ □ □□ □□.
2. 2004□ □□ □□ □□□ □□ □□ □□ □□.
3. 2004□ □□ □□ □□□ □□□ □□□ □□ □□.
4. 2004□ □□ □□ □□□ □□ □□ □□ □□ □□.

A. 1, 2, 3□
B. 1, 2, 4□
C. 1, 3, 4□
D. 2, 3, 4□
Answer: (SHOW ANSWER)
According to the CAMS study guide, chapter 4, page 1191, transaction records include any records that reflect the movement of funds or assets, such as wire transfers, checks, deposits, withdrawals, securities trades, etc. Therefore, items 1, 2, and 4 are examples of transaction records that should be delivered in response to a legal request. Item 3, signature cards, are not transaction records, but rather account opening documents that contain the customer's name, address, identification, and signature. These documents may be relevant for customer due diligence or identification purposes, but they do not reflect the transaction activities of the customer.
Reference:
1: ACAMS CAMS Study Guide - 6th Edition, Chapter 4, page 119: https://www.acams.org/wp-content/uploads/2019/09/ACAMS-CAMS-Study-Guide-6th-Edition-Chapter-4.pdf

NEW QUESTION: 176
□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□□. □□ □ □□ □□□ □□□□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□□□□□ □□
B. □□□□□□ □□
C. □□ □□
D. CEO□ □□ □□
Answer: (SHOW ANSWER)
The most important consideration when deciding whether to recommend closing the account is the institution's anti-money laundering policy. This is because the policy should provide clear and consistent criteria for account closure decisions, based on the risk assessment, the nature and severity of the suspicious activity, the customer due diligence information, and the legal and regulatory obligations of the institution. The policy should also ensure that the account closure process is independent, objective, and transparent, and that it does not compromise the confidentiality of the suspicious transaction report or the investigation.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 5, Section 5.4.2, page 1971 ACAMS CAMS Certification Video Training Course, Module 5, Lesson 5.4, video time 9:00-10:302 ACAMS CAMS Certification Practice Exam, Question 145, page 2863

NEW QUESTION: 177
□□ □□□ □□□ □□ □□□ □□ □□ □□□ □□□. □□□□ □□□ □□□ □□ □□ □□ (□□□)□□ □□□ □□□ □□□□□. □□□ □□ □□ □□□□□ □□ □□□ □□□□ □□ □□□. □□ □ □ □□□ □□ □ □□□□ □□ □□□□□?

A. □□□□
B. □□□
C. □□
D. □□ □
Answer: D (LEAVE A REPLY)
The account officer has violated the principle of confidentiality by informing the customer about the legal request from law enforcement. This could amount to tipping off, which is a criminal offense in many jurisdictions. Tipping off could jeopardize the investigation, compromise evidence, and alert other potential suspects. The account officer should not discuss any details of the investigation with the customer, nor should he meet with the customer to do so. He should also report his actions to his manager and compliance department, and cooperate with law enforcement as required.
Reference:
ACAMS CAMS Certification Video Training Course1, Module 4: Conducting or Supporting the Investigation, Lesson 4.3: Confidentiality and Information Sharing ACAMS CAMS Certification Study Guide2, Chapter 4: Conducting or Supporting the Investigation, Section 4.3: Confidentiality and Information Sharing, pp. 135-136 ACAMS CAMS Certification Exam Outline3, Domain 4: Conducting or Supporting the Investigation, Task 4.3: Maintain confidentiality of the investigation, p. 18

NEW QUESTION: 178
□□□ □□□ □□ □□□ □□(EDD)□ □□□ □□ □□□ □□□□ □□□?
A. □□ □□□ □□□ □□ □□
B. □□□ □□□□ □□□ □□ □□ □□
C. □□ □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
According to the CAMS Study Guide, EDD is a higher level of scrutiny applied to customers who pose a greater risk of money laundering or terrorist financing. EDD may include obtaining additional information on the customer's identity, source of funds, business activities, beneficial owners, and expected transactions. Details on individuals with control over the account are relevant for EDD, as they may indicate the involvement of politically exposed persons (PEPs), sanctioned individuals, or other high-risk entities. Therefore, this information should be gathered as part of EDD for a high-risk customer.

NEW QUESTION: 179
□□□□□ □□□□ □□ □□□ □□□□. □□ □ □□ □□ □□□ □□ □□ □□ □□□ □□ □□ □□ □□□□□?
A. □□□□□ □□□ □□□ □□□ □□ □□ □□.
B. □□□□□ □□□ □□□□ □□□ □□ □□□.
C. □3□□□□ □□□□□ □□ □□□ □□ □□□□□.

D. □□□□□□ □□ □□□□□ □□ □□□□□□.

Answer: (SHOW ANSWER)

This represents the highest risk factor for terrorist financing because it may indicate that the charity is diverting funds to support terrorist organizations or activities, or that it is acting as a front or conduit for terrorist financing. Disbursement of funds to entities unrelated to the purpose of the charity may also violate the donor's intentions, the charity's mission, or the applicable laws and regulations. A charity with unaudited accounts may have weak internal controls, governance, or transparency, which may increase the risk of misappropriation, diversion, or misuse of funds.

Reference:

ACAMS CAMS Certification Video Training Course1, Module 2: Money Laundering Risks and Methods, Lesson 2.3: Money Laundering Risks and Methods by Sector ACAMS CAMS Study Guide, 6th Edition2, Chapter 2: Money Laundering Risks and Methods, Section 2.3: Money Laundering Risks and Methods by Sector, pp. 40-41 ACAMS CAMS Examination Preparation Seminar, 6th Edition3, Chapter 2: Money Laundering Risks and Methods, Section 2.3: Money Laundering Risks and Methods by Sector, Slide 18

NEW QUESTION: 180

□□□ □□ □□ □□ □□□ □□□□□□ □□□□□□ □□□□□ □□ □□□ □□□ □□□□□□ □. □□□ □□ □□□ □□ □□□□□ □□□□□ □□□□□ □□□□□□ 80□ □□ □□□ □□□ □□ □□ □□□□□□. □□□□□ □□ □□□ □□ □□□ □□□□□ □□□? (3□□ □□□□□□.)

A. □□□

B. □□□

C. □

D. □□ □□

E. □□□

F. □□□□ □□

Answer: C,E,F (LEAVE A REPLY)

The scenario described in the question presents several indicators of potential money laundering through real estate, which the broker should be aware of and report accordingly. The most relevant red flags are:

Value: The student wants to buy a home that is overvalued, meaning that the asking price is higher than the market value or the appraisal value of the property. This could indicate that the student is trying to launder a large amount of illicit funds in one transaction, or that the seller is colluding with the student to inflate the price and receive a kickback. Overvaluing or undervaluing properties is a common technique used by money launderers to manipulate the price of real estate and conceal the source or destination of their funds12.

Inconsistency: The student's behavior and profile are inconsistent with the typical characteristics of a legitimate home buyer. The student cancels the viewing of the home at the last minute due to illness, which could suggest a lack of interest or a pretext to avoid scrutiny. The student also wants to buy an expensive home despite being a student, which could indicate a discrepancy between the student's income and the source of funds. Moreover, the student disregards the

broker's objections to the asking price, which could imply that the student is not concerned about the value or quality of the property, but rather the amount of money that can be laundered through it34.
Transaction speed: The student wants to quickly buy the home, which could indicate a sense of urgency or pressure to move the illicit funds before they are detected or seized by the authorities. Money launderers often use fast transactions to avoid raising suspicion or leaving a paper trail. Transaction speed is especially relevant when combined with other red flags, such as cash payments, anonymous buyers, or overvalued properties5 .
Reference:
Understanding Money Laundering in Real Estate
RED FLAG INDICATORS FOR REAL ESTATE SECTOR
Investigating Money Laundering through Real Estate
AML Red Flags Associated with Real Estate Sector Businesses
FinCEN Proposes Rule to Combat Money Laundering and Promote Transparency in Residential Real Estate
[ACAMS Study Guide, 6th Edition, Chapter 7, pp. 200-201]

NEW QUESTION: 181
□□□ □□□ □□□ □□□ □□ □□□ □□□□□. □□□ □□□ □□□ □□ □□ □□□□□. □□□ □□ □□□ □□□□. □□ □□□ □□□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□ □□□□.
□ □□□ □□□□ □□ □ □□ □□□ □□ □ □□ □□□ □□□ □□□? (□ □□□ □□□□□.)
A. □□ □□□□ □□□□ □□□□□.
B. □□□ □ □□□ □□□ □□□ □□□ □□□□□.
C. □□□□ □□□□□ □□□ □□□ □□□ □□□□ □□□ □□□□□ □□□□□.
D. □□ □□□□□□□ □□□ □□□□□ □□ □□ □□□ □□□□□.
Answer: A,C (LEAVE A REPLY)
Units
Explanation:
The correct answer is A and C. Law enforcement should determine who are the signatories on the account and examine the flow of money from the company to the individual in an effort to determine if it is legitimate. These steps would help to identify the source and destination of the funds, the purpose and nature of the transactions, and the possible involvement of money laundering or other financial crimes. Asking the bank for the history of the multi-level marketing company (B) may not be relevant or useful, as the company may have a legitimate business model or a false front. Examining possible Suspicious Activity Report information received from the local Financial Intelligence Units (D) may be helpful, but it is not a necessary step, as the bank may not have filed any reports or the reports may not contain sufficient information.
Reference:

ACAMS CAMS Certification Video Training Course1, Module 4: Conducting or Supporting the Investigation Process, Lesson 1: Investigating Techniques for Law Enforcement ACAMS CAMS Certification Study Guide2, Chapter 4: Conducting or Supporting the Investigation Process, Section 4.1: Investigating Techniques for Law Enforcement, pp. 125-126

NEW QUESTION: 182

FATF □□□ 29□ □□□ □□□□□□□(FIU)□ □□ □□□ □□ □ □□□□□□?

A. □□□□□□ □□□ □□□□□ □□□□□ □□□ □□ □□□□ □□□.

B. □□ □□□ □□□ □□□□□□□ □□□□□□□□ □□ □□□□ □□□ □□□□□□.

C. AML □□□ □□ □□ □□ □□ □□□□ □□ □ □□ □□.

D. □□ □ □□ □□□□□ □□□□ □□□□ □□ □□□□ □□ □□□□ □□□□□□.

Answer: A (LEAVE A REPLY)

A Financial Intelligence Unit (FIU) acts as the central hub for AML/CFT intelligence in a country.

Option A (Correct): FIUs collect, analyze, and disseminate financial intelligence related to suspicious transactions to law enforcement and regulators.

Option B (Incorrect): FIUs do not prosecute cases; they refer cases to law enforcement for prosecution.

Option C (Incorrect): FIUs analyze data but do not develop surveillance technology.

Option D (Incorrect): FIUs share intelligence with authorized entities, but not real-time criminal data with the private sector.

Types of FIUs:

FIU Model Description Example

Administrative FIU Operates under a government agency or central bank. FinCEN (USA), AUSTRAC (Australia) Law Enforcement FIU Operates within a law enforcement body. UK NCA (UK), IMPA (Israel) Judicial FIU Operates within a judicial authority. Belgium CTIF-CFI Why FIUs Are Important:

They bridge the gap between banks, regulators, and law enforcement.

They ensure confidential handling of SARs.

They support domestic and international cooperation in AML/CFT efforts.

Reference:

FATF Recommendation 29 (FIUs)

Egmont Group Guidelines on FIU Cooperation

EU Directive on the Role of FIUs

NEW QUESTION: 183

□□ □□ □□ □□□ □□□ □□□ □□ □ □□ □□□ □□□ □□□ □ □□ □□ □□□ □□□?

A. □□□ □ □□□□□ □□□ □□□□□□.

B. □□□ □□□□□□ □□□ □□□□□□ □□ □□□□□□.

C. □□ □□□□□ □□□ □□□□□ □□□□.

D. □□□ □□□ □□□ □□□ □□□ □ □□□□.

Answer: A ([LEAVE A REPLY])

it describes a reason why trusts established in certain offshore jurisdictions make good vehicles to layer money, which is names of the settlor and beneficiaries are not publicly available. This means that the true owners and controllers of the funds or assets held by the trust are hidden from the public and the authorities, and can only be accessed by the trustee or the protector, who may be complicit or unaware of the money laundering scheme. This creates a high level of anonymity and secrecy for the money launderers, who can use the trust to move, disguise, or conceal the origin and destination of their illicit funds.

The other options are not necessarily reasons why trusts established in certain offshore jurisdictions make good vehicles to layer money, although they may have some advantages or disadvantages depending on the circumstances and the risk profile of the customers and countries involved. Option B describes a possible motive for setting up a trust in an offshore jurisdiction, which is to minimize taxes, but this does not imply that the trust is used to layer money, as there may be legitimate tax planning or optimization purposes. Option C describes a possible challenge or obstacle for setting up a trust in an offshore jurisdiction, which is offshore jurisdictions are unfamiliar with trust, but this does not imply that the trust is used to layer money, as there may be other legal or financial vehicles available in those jurisdictions. Option D describes a possible characteristic or feature of a trust, which is trusts may hold assets of significant size, but this does not imply that the trust is used to layer money, as there may be valid reasons or sources for the large assets.

Reference:

ACAMS CAMS Certification Video Training Course - 6th Edition1

Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)2 ACAMS CAMS Study Guide - 6th Edition, Chapter 4, pages 86-87

: https://www.acams.org/wp-content/uploads/2019/09/ACAMS-CAMS-Study-Guide-6th-Edition-Chapter-4.pdf

NEW QUESTION: 184

□□ □□□ AML □□ □□□ □□□□□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□□□ □?

A. □□□□ □□

B. □□ □□

C. □□

D. □□□□ □□

Answer: A (LEAVE A REPLY)

Non-compliance with AML regulatory obligations can have severe consequences for financial institutions. Among these, the most severe consequence is the loss of license. When a financial institution fails to meet AML requirements, regulators may revoke its license to operate. Losing the license effectively shuts down the institution's ability to conduct business, impacting its existence and operations significantly12.

Reference:

1. Unit21 AML: 8 AML Penalties, Fines, and Sanctions + Examples You Should Avoid
2. Financial Crime Academy: Ensuring Compliance: The Power Of AML Regulatory Reporting

NEW QUESTION: 185

OFAC(□□□□□□□)□□ □□□ □□□ □□ □ □□□ □□ □□□□ □□□ □□□□□? (2 □□ □□□□□.)

A. □□□ □□ □□□ □□ □□□ □□□□ OFAC □□□□ □□□□□.

B. □□ □□□ □□ □□□ □□ OFAC □□□ □□□□ □□□.

C. □□ □□□ □□□ □□□□ □□□□ OFAC □□□ □□□ □ □□□ □□□□.

D. □□ □□□ OFAC □□□ □□ □□ □□□ □□□ □□□□ □□□□ □□□ □□□□.

E. □□□ □□□ □□ □□ □□□ □□□ OFAC □□□ □□□ □□□ □□□□.

Answer: B,D (LEAVE A REPLY)

The rules imposed by the Office of Foreign Assets Control (OFAC) for legal entities and persons related to the US are:

Nationals of the US must comply with OFAC rules, regardless of where they are located in the world. This means that US citizens, permanent residents, and entities organized under US law are subject to OFAC sanctions and prohibitions, even if they operate or reside outside the US12.

Any foreign corporation is also penalized if it conducts transactions with sanctioned countries under OFAC rules. This means that non-US entities that engage in trade or financial dealings with OFAC-designated countries, entities, or individuals are liable to face civil or criminal penalties, as well as secondary sanctions that could restrict their access to the US market or financial system34.

The other options are not correct, because:

A subsidiary of a legal entity of the US, which is formally registered in a foreign country, is not exempt from OFAC rules. This means that foreign-incorporated entities that are owned or controlled by US persons or entities are also subject to OFAC sanctions and prohibitions, unless they are specifically authorized or licensed by OFAC12.

A foreign individual visiting the US for a short vacation is not obligated to follow OFAC rules. This means that non-US persons who are temporarily present in the US are not subject to OFAC sanctions and prohibitions, unless they are involved in transactions that have a US nexus or violate other US laws.

The head office of a foreign legal entity which has a branch in the US does not need to comply with OFAC rules. This means that non-US entities that have a presence or operation in the US are not subject to OFAC sanctions and prohibitions, unless they are involved in transactions that have a US nexus or violate other US laws.

Reference:

ACAMS CAMS Certification Video Training Course - Exam-Labs3

Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)4 ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 7, page 147: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-7.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 7, page 148: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-7.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 7, page 149: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-7.pdf

NEW QUESTION: 186

□□□□□ A□ □□ □□ □□ □□□ □□ □□□□ □□□□□. □□ □□□ □□ □□□□□ A □ □□□□□ □□□ □□□□□□ □□□□□ □□□ □□□ □□ □□□ □□□□□□. □□□ □□ □□ □□□□ □□□ □ □□□□ □□□□ □□ □□□ □□□ □□□?

A. □□□□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□□.

B. □□□□ □□□□ □□□ □ □□□ □□ □□ □□ □□□ □□□□□□ □□ □□□□□.

C. □ □□ □□□ □□□ □□□ □□□ □□□ □□□□□ □□□□□.

D. FBI(Federal Bureau of Investigation)□ □□□□ □□ □□□ □□□□□□.

Answer: A (LEAVE A REPLY)

After filing a suspicious activity report (SAR), an investigator should prepare a summary for senior management recommending client off-boarding. This is because client off-boarding is a risk-based decision that requires senior management approval and may involve legal considerations. Informing other local financial institutions about the client, restraining or blocking the client's account(s), or contacting law enforcement directly are not appropriate actions for an investigator to take after filing a SAR, as they may compromise the confidentiality of the SAR, violate privacy laws, or interfere with ongoing investigations.

NEW QUESTION: 187

□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□□?

A. □□ □ □□□ □□ □□□ □□ □□

B. □□ □□□□ □□□□□ □□ □□□□ □□

C. □□□□□□ □□□□ □□□ □□ □□ □□□□□□ □□

D. □□ □□□□ □□□ □□□□□ □□□ □ □□ □□ □□

Answer: D (LEAVE A REPLY)

concern

Explanation:

Section 311 of the USA PATRIOT Act grants the Secretary of the Treasury the authority to designate foreign jurisdictions, financial institutions, classes of transactions, or types of accounts as being of primary money laundering concern, and to impose one or more of five special

measures on them. These special measures range from requiring enhanced recordkeeping and reporting to prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for the designated entities. The purpose of these special measures is to protect the U.S. financial system from money laundering and terrorist financing risks posed by the designated entities.
Reference:
USA PATRIOT Act | FinCEN.gov
FACT SHEET for Section 312 of the USA PATRIOT Act Final Regulation and Notice of Proposed Rulemaking | FinCEN.gov International Financial Crime: Treasury's Roles and Responsibilities Should Be Updated - GovInfo

NEW QUESTION: 188
□□ □□□(USA PATRIOT Act)□ □□ □□□ □□ □□□ □□□ □ □□ □□(FIs)□ □□ □□ □□□ □□ □ □□□ □□□□□?
A. □□ □□ □□ □□□ □□ □□□ FI□ □□ □□ □□ □ □□□ □□□ □□□ □ □□□ □ □□□□.
B. □□□ □□□□ □□ FIs□ □□□ □□.
C. □□ □□□ □□□□ □□ □ FI□ □□ □□□□□ □□□□□.
D. □□ FI□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□.
Answer: (SHOW ANSWER)
Section 319(b) of the USA PATRIOT Act authorizes the U.S. government to subpoena records from any foreign bank that maintains a correspondent account in the U.S., regardless of whether the foreign bank has a physical presence in the U.S. or not. The subpoena may request any records relating to the correspondent account or any account at the foreign bank, including records maintained outside the U.S. If the foreign bank fails to comply with the subpoena, the U.S. government may direct any U.S. financial institution to terminate its correspondent relationship with the foreign bank and impose civil penalties.
Reference:
Bank Records Related to Anti-Money Laundering Programs, FinCEN, accessed February 2024.
How Patriot Act Affects Financial Institutions?, Sanction Scanner, November 2020.

NEW QUESTION: 189
□ □□□ □□□ □□□□ □□□□ □□□□ □□□ □□, □□ □□ □□ □□ □□ □□, □□ □□ □□ □□, □□□□ □ □ □□□□ □□ □□□□□ □□□□□ □□ □□ □ □□□ □□□ □□ □□ □□□ □□□□ □□□□. □□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□ □□?
A. □□ □ □□□ □□
B. □□□□ □ □ □□□□ □□ □□□□ □□□□□ □□□ □□□□□.
C. □□□ □□□ □□
D. □□□□ □□ □□
Answer: (SHOW ANSWER)

Financing terrorism generally refers to providing money or other support, such as personnel or technology, to terrorist activities. This can include providing funds to terrorist networks, providing services to support terrorist operations, and providing resources to support terrorist activities. In this case, paying producers and reporters for television and web messaging would be considered financing of terrorism, as it is providing support for terrorist activities.

NEW QUESTION: 190

Financial Action Task Force 40 Recommendations□ □□ □□□ □□ □□ □□ □□□ □□□ □ □□ □□□ □□□ □□□?

A. □□

B. □□

C. □□□□

D. □□□□□

Answer: D (LEAVE A REPLY)

The FATF 40 Recommendations are the international standards for combating money laundering, terrorist financing, and proliferation financing. They provide a comprehensive and consistent framework of measures that countries should implement in their national systems.
Recommendation 5 of the FATF 40 Recommendations states that countries should criminalize the financing of terrorism, terrorist acts and terrorist organizations. This means that countries should adopt laws that make it an offence to provide or collect funds or other assets with the intention or knowledge that they will be used to carry out terrorist acts or support terrorist organizations. Countries should also ensure that such offences are punishable by effective, proportionate and dissuasive sanctions. Furthermore, countries should ensure that terrorist financing offences extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts or support terrorist organizations. Therefore, the correct answer is D. Criminalize, as this is the action that countries should take related to the financing of terrorist acts in accordance with the FATF 40 Recommendations.

Reference:
FATF website
FATF 40 Recommendations - February 2012
FATF Recommendation 5 - Criminalisation of Terrorist Financing
feb-2019.html

NEW QUESTION: 191

□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□ □□(PEP)□ □□□□ □□□ □□□□. □□□ □ □□ □□□ □□□□□?

A. □□□ □□ □□□□□ □□□□.

B. PEP□ □ □ □□□ □ □□□ □□ □□ □□□□□ □□□□□.

C. □□ □□ □□□ PEP□ □□ □□ □□□ □□□ □□□.

D. □□ □□□ □□□□ □□ □□ □□(FI)□ □□ PEP □□□ □□□□□.

Answer: A (LEAVE A REPLY)

According to the ACAMS CAMS Study Guide, one of the key elements of an effective anti-money laundering (AML) program is ongoing training for all relevant staff. Training should cover the legal and regulatory obligations, the risks and red flags of money laundering and terrorist financing, the procedures and controls for customer due diligence and transaction monitoring, the reporting and record-keeping requirements, and the roles and responsibilities of the staff and the management. Training should also be tailored to the specific functions and needs of the staff, and should be updated regularly to reflect the changes in the AML environment and the FI's policies and procedures.

PEPs are considered high-risk customers for AML purposes, as they may abuse their positions of power and influence to commit or facilitate corruption, bribery, embezzlement, or other financial crimes. Therefore, it is essential that the FI's staff are aware of the definition and categories of PEPs, the sources and methods to identify and verify PEPs, the enhanced due diligence measures and ongoing monitoring that apply to PEPs, and the escalation and reporting procedures for suspicious activities involving PEPs .

If an internal audit reveals that a large group of employees do not know how to handle PEPs, this indicates a serious gap in the FI's AML training program, which could expose the FI to regulatory sanctions, reputational damage, and legal liabilities. Therefore, the next course of action that should be taken is to create a company-wide training program that covers the relevant aspects of PEPs, and to ensure that the training is delivered to all staff who deal with PEPs or have access to PEP-related information. The training should also be evaluated for its effectiveness and impact, and the results should be reported to the senior management and the board of directors.

Reference:

: ACAMS CAMS Study Guide, 6th Edition, Chapter 2: Developing an Effective Anti-Money Laundering Program, page 51-52

: ACAMS CAMS Study Guide, 6th Edition, Chapter 3: Conducting Customer Due Diligence, page 75-78

: FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22), June 2013, 1

: ACAMS CAMS Study Guide, 6th Edition, Chapter 4: Conducting Ongoing Monitoring, page 97-98

NEW QUESTION: 192

□□□ □□□ □□□ □ □□□ □□□□□. □□ □□□ □□ AML □□□ □□□□ □□ □□ □ □□□□?

A. □□□□□ □□□□□□ □□□ □□□□□ □□□□ □□□ □□□ □□.

B. □□□□ □□ □□□ □□□□ □ □ □□ □□□ □□□□□.

C. □□□ □□□ □□□ □□□ □□□ □□ □□ □□□□□□ □□ □□.

D. □□□□ □□□ □3□□□□□ □□ □□ POS □□.

Answer: B (LEAVE A REPLY)

payments received on the account that reference unknown companies in the instructions indicate a possible attempt to obscure the source or purpose of the funds. This could be a sign of money laundering, tax evasion, fraud, or other illicit activities. Such payments should be referred to AML Investigations for further review and verification of the identity and legitimacy of the companies involved.

Reference:

FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones, page 18, paragraph 57: "The dealer should also pay attention to the information provided by the customer on the source and origin of the funds or assets, and verify it where possible. For example, the dealer should be alert to situations where the customer provides vague, incomplete or inconsistent information about the source and origin of the funds or assets, or where the information provided does not match with the customer's profile or business activity." Risk-Based Approach For Dealers in Precious Metals and Stones (DPMS), section "Business-based risk approach", sub-section "2- Geographical location": "You must also assess the geographical location of your business and the countries you deal with. You must be aware of the countries that are high-risk or non-cooperative jurisdictions as per the FATF recommendations. You must also consider the countries that are subject to sanctions, embargoes, or similar measures issued by the United Nations, the European Union, or any other relevant organization. You must also be careful of the countries that are known to have significant levels of corruption, organized crime, or terrorist activity." What are the Risks of Money Laundering for Precious Metals Dealers?, section "Money Laundering Red Flags for DPMS", bullet point 4: "The customer provides vague, incomplete, or inconsistent information about the source and origin of the funds or assets."

NEW QUESTION: 193

□□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□?

A. □□□ □□□□ □□

B. □□ □□ □□□ □□□□ □□

C. □□□ □□ □□□ □□□□ □□

D. □□□ □□□□□□ □□□ □□

Answer: B (LEAVE A REPLY)

"Increasingly, countries are using economic sanctions instead of military force as an instrument of foreign policy"

NEW QUESTION: 194

□□ □□ □□ □□ □□ □□□□□ □□□□ □□ □□□□□ □□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□□□. □ □□□ □□ □□ □□□ □□ □□ □□ □□ □□ □□□ □□□□□□. □□□□□□ □□□□ □□ □□ □□ □ □□

A. □□ □□□ □□□ □□ □□ □□□ □□ □□ □□ □□ □□□ □□□□□.

B. □□□ □□ □□ □□ □□ □□□ □□ □□ □□□ □□□□□.

C. □□□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□ □□ □□□□ □□□□□.

D. □□ □□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

The first thing the anti-money laundering specialist should do is to conduct a risk assessment of the bank's international electronic fund transfer activity. This is to identify and measure the potential money laundering and terrorist financing risks associated with the bank's products, services, customers, and geographic locations. A risk assessment can help the anti-money laundering specialist to:

Understand the nature and extent of the bank's exposure to money laundering and terrorist financing threats and vulnerabilities.

Establish a risk-based approach to the design and implementation of the anti-money laundering compliance program, including policies, procedures, controls, monitoring, reporting, and training.

Allocate appropriate resources and prioritize actions to mitigate the identified risks and enhance the effectiveness of the anti-money laundering compliance program.

Demonstrate to the regulators and auditors that the bank has a sound and comprehensive anti-money laundering compliance program that is commensurate with its risk profile and business activities.

Reference:

CAMS Study Guide - 6th Edition, Chapter 6, pages 167-168

CAMS Certification Exam Outline, Domain 3, Task 3.1, Skill 3.1.1

Anti-Money Laundering Bulletin November 2021 - Central Bank of Ireland, pages 4-5 Money Laundering through Money Remittance and Currency Exchange Providers, FATF, June 2010, pages 7-8 REGULATIONS - FIU, Part III, Regulation 9, pages 9-10

NEW QUESTION: 195

OFAC□ □□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□□.

A. □□□ □□ □□ □ □□ □□ □□□ □□□□□.

B. □□□ □□□□□ □□□□□ □□ □□□□□□ □□□ □□□□□.

C. □ □□□□ □□□ □□□□□□ □□□ □□□□ □□□□□.

D. OFAC □ □□ □□□ □□ □ □□ □□ □□□ □□□□□□.

Answer: A (LEAVE A REPLY)

The Office of Foreign Assets Control (OFAC) is a department of the US Treasury that administers and enforces economic and trade sanctions imposed by the US against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. The main purpose of the US Treasury Department for OFAC's extraterritorial reach is to apply these sanctions to any person or entity that is subject to US jurisdiction, or that engages in transactions involving US persons, US dollars, or US goods or services. This way, the US can exert pressure on the targets of the sanctions and prevent them from accessing the US financial system or market. OFAC's extraterritorial reach is authorized by Congressional legislation or presidential emergency powers, and is often based on UN Security Council resolutions or multilateral agreements.

Reference:

Office of Foreign Assets Control (OFAC): Definition, Sanctions
About OFAC | Office of Foreign Assets Control
OFAC's Extraterritorial Reach: Purpose of the US Treasury Department

NEW QUESTION: 196
AML □□□ □□□ □ □□□□□ □□□□□ □ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□
□?
A. □□□ AML□ □□□ □□ □□□□□ □□□□□ □□□ □□□ □□□ □□□ □□□ □□ □□
□.
B. AML□ □□□ □□ □□□□□ □□□□□ □□ □□□□□□□□ □ □□□.
C. □□ □□ □□ □□ □□ □□□□□ □□ AML □□□□ □ □□□□□□.
D. □□ □□ □□□ □□□ □□ □□□□□ □ □□□□□ □□□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
An auditor who performs an AML investigation should adhere to the principle that AML and Data Protection Privacy laws should not be mutually exclusive. This means that the auditor should respect and protect the personal data of the individuals involved in the investigation, while also complying with the AML obligations and requirements. The auditor should balance the legitimate interests of preventing and detecting money laundering and terrorist financing with the fundamental rights and freedoms of the data subjects, and apply the data protection principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.
The auditor should also take into account the relevant legal frameworks and guidance on data protection and AML, such as the EU General Data Protection Regulation (GDPR), the EU Anti-Money Laundering Directive (AMLD), the Council of Europe Convention 108+ on data protection, and the Guidelines on data protection for the processing of personal data for AML/CFT purposes issued by the Consultative Committee of the Convention 108+. The auditor should also cooperate and consult with the data protection authorities and the AML authorities, as appropriate, to ensure compliance and consistency.
Reference:
Data protection and the EU's anti-money laundering regulation
The EU's anti-money laundering regulation and data protection: Part II
For Banks, Data Privacy and Anti-Money Laundering Don't Have to Be Incompatible Guidelines on data protection for the processing of personal data for AML/CFT purposes Data Protection requirements must go hand in hand with the prevention of money laundering and terrorism financing ACAMS CAMS Certification Study Guide 6th Edition

NEW QUESTION: 197
□□ □□□ □□□□□□□ □□ □□□ □□□ □ □□ □□□ □□ □□ □□□ □ □□ □□□ □ □□ □□□ □ □□ □ □□ □□□ □□□ □□□? (2□□ □□□□□.)
A. □□ □□□□ □□ □□ □□ □□□ □□
B. □□ □□ □ □□ 5□ □□ □□ □□ □□
C. □□□ □□□□ □ □□ □□□ □□ □□□ □□
D. □ □□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□ □□□ □□□□□.
Answer: B,C (LEAVE A REPLY)
According to the Anti-Money Laundering Specialist (the 6th edition) study guide, when a financial institution receives a law enforcement request to keep an account open that may be associated with suspicious or criminal activity, it should take the following two steps:
Maintain account records for at least five years after the request expires. This is to ensure that the financial institution can provide evidence of its compliance with the law enforcement request and the applicable anti-money laundering regulations. The five-year retention period is based on the international standard set by the Financial Action Task Force (FATF) and adopted by many jurisdictions12.
Ask for a written request from the law enforcement agency that defines the duration. This is to protect the financial institution from potential liability and to clarify the scope and purpose of the law enforcement request. The written request should specify the time period for which the account should remain open, the reason for the request, the contact information of the law enforcement officer, and the legal authority for the request34.
Reference:
Anti-Money Laundering Specialist (the 6th edition) study guide, page 57 FATF Recommendation 11, paragraph 2 Anti-Money Laundering Specialist (the 6th edition) study guide, page 58 Money Laundering website, article on "Law Enforcement Requests to Keep Accounts Open" https://www.fincen.gov/resources/statutes-regulations/guidance/requests-law-enforcement-financial-institutions-maintain

NEW QUESTION: 198
□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□ □□□ □□ □ □□□ □□□□□?
A. □□ 319(b)
B. □□ 314(b)
C. □□ 314(a)
D. □□ 319(a)
Answer: (SHOW ANSWER)
Section 319(b) of the USA PATRIOT Act allows U.S. authorities to seize funds from correspondent accounts held by foreign banks in the U.S.

Option A (Correct): Section 319(b) grants the U.S. government authority to seize assets in U.S. correspondent bank accounts belonging to foreign financial institutions involved in illicit activities.
Option B (Incorrect): Section 314(b) facilitates voluntary information sharing among financial institutions but does not authorize asset seizure.
Option C (Incorrect): Section 314(a) relates to law enforcement requests for financial intelligence, not asset seizures.
Option D (Incorrect): Section 319(a) concerns record-keeping requirements for foreign banks but does not authorize asset seizures.
Best Practices for Foreign Banks with U.S. Correspondent Accounts:
Ensure full AML compliance to avoid regulatory scrutiny.
Avoid processing high-risk transactions that may trigger U.S. jurisdiction.
Monitor cross-border transactions to detect potential financial crime exposure.
Reference:
USA PATRIOT Act Section 319(b) (Correspondent Banking Asset Seizures)
FinCEN Guidance on Extraterritorial AML Compliance
FATF Recommendation 13 (Correspondent Banking AML Risks)

NEW QUESTION: 199
FATF□ CDD(□□ □□) □□□□□□ □□□ □□ □ □□ □□□ □□□ □□ □□□□□□.
A. □□ □ □□□□□ □□ □□ □□□ □□□□□□.
B. □□□□□ □□□ □□ □□□□□ □□□ □□□□□ □□□ □□□□□□□□.
C. □□ □ □□□ □ □□□ □□ □□□□□ □□□□□□.
D. □□□□□ □□ □□□□□ □ □□.
Answer: B (LEAVE A REPLY)
According to the FATF Recommendation 10, financial institutions should conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. This is one of the core measures of customer due diligence (CDD) that aim to prevent and detect money laundering and terrorist financing risks.

NEW QUESTION: 200
□□ □□□ □□ □□□□□ □□ □□□ □□□ □□□ □, □□□□ AML/CFT □□ □ □□ □□ □ □□□□□ □ □□ □□□□□ □□□ □□□□□ □□□□?
A. □□□□□□□□(COO)
B. □□□
C. AML □□ □□ □□□ □□
D. □□□□□□(CEO)
Answer: B (LEAVE A REPLY)
The Board of Directors holds ultimate responsibility for AML/CFT compliance and governance.
Option B (Correct): The Board must oversee, approve, and ensure AML programs are effective.

Option A (Incorrect): The COO manages operations, but does not hold ultimate accountability.
Option C (Incorrect): While the AML officer executes compliance programs, the Board provides oversight.
Option D (Incorrect): The CEO is responsible for strategy, but AML failures fall under Board accountability.

NEW QUESTION: 201

□□ □□□ FATF(Financial Action Task Force) □□ □□ □□□□ □□□ □□□ □□ □□ □□□□ □□□□ □□ □□□□□□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□ □□ □□ □□□(CCO)□□ □□□□□□. (□□). CCO□ □□□ □□□□ □□□?

A. □ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □ □□□ □□ □ □□ □□□ □□□ □ □□□□.

B. MER□ □□□□ □□ □□. □□□□ FATF□ □□□□□ MER□ □□□□ □□ □□□ □□ □□□□ □□□ □□□ □□ □□□□□□.

C. MER□ □□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□ □□□ □□ □□ □ □□□ □□□ □□□□□.

D. □□ □□□ □□□ □□ □□ □ □□□□□ □□ □□ □□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□.

Answer: A ([LEAVE A REPLY])

According to the Certified Anti-Money Laundering Specialist (the 6th edition) Study guide, the CCO should advise the manufacturing customer that increased scrutiny of cross-border transfers may lead to delays and caution them to ensure that all necessary documentation is provided in order to facilitate a timely transfer. Additionally, the CCO should recommend that the customer contact the FATF to discuss the possibility of an independent review of the findings, as well as other options to mitigate the potential negative consequences.

NEW QUESTION: 202

□□(□□) □□□ □□ □ □□ □□□□ casas de cambio□ □□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□. □□□ □□□ □□□□□□ □□ □□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□□.

□□□□ □ □□□ □□ □□ □□□ □□ □□□ □□□□□ □□ □ □□□ □□□ □□□? (2 □□ □□□□□.)

A. □□□□□□ □□ □ □□□□□□□ □□

B. □□□□ casas de cambio□ □□ □□ □□ □□□ □□ □□ □□ □□

C. □□□□□ □□□ □□□ □□ □□□ □□□ □3□ □□□ □□□□ casas de cambio□ □□ □□ □□

D. casas de cambio□ casa de cambio□ □□□ □□□□ □□□ □□ □□□ □□□ □□ □□ □□ □□□ □□ □□ □□□ □□□□□.

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

According to the ACAMS Study Guide 6th Edition, Chapter 2, page 38, one of the steps that a financial institution should take when it suspects money laundering activity is to file a suspicious

transaction report (STR) or a suspicious activity report (SAR) to the relevant authorities. This will alert the regulators and law enforcement of the potential money laundering scheme and provide them with valuable information to trace the funds and identify the perpetrators.
Another step that a financial institution should take is to identify any unusual or suspicious wire transfers initiated by casas de cambio to jurisdictions outside of Mexico that bear no apparent business relationship with that casa de cambio. This could indicate that the casas de cambio are involved in layering and integration stages of money laundering, where they are moving the illicit funds across borders and disguising their origin and ownership. The financial institution should monitor and document these wire transfers and report them to the authorities if necessary.
Option B is not a relevant step to trace funds through the bank, as it does not provide any information about the source, destination, or purpose of the funds. A decrease in the sale of large denomination U.S. bank notes to casas de cambio by the bank could be due to various factors, such as market demand, exchange rates, or regulatory changes, and does not necessarily indicate money laundering activity.
Option C is also not a relevant step to trace funds through the bank, as it does not indicate any connection to the suspected money laundering scheme. Deposits by casas de cambio that include third-party items, such as sequentially numbered monetary instruments, could be legitimate transactions that are part of the normal business operations of the casas de cambio. Unless there is evidence that these deposits are related to the sale of large denomination U.S. bank notes or the Mexican syndicate, they are not useful for tracing the funds.
Reference:
ACAMS Study Guide 6th Edition, Chapter 2, page 38
Combating Money Laundering and Other Forms of Illicit Finance
Sting Operation Snares Casa de Cambio for Allegedly Laundering Millions Through U.S. Banks

NEW QUESTION: 203
□□□ □□□□□□ □□□□ □□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□. □□□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□. □□ □□□□ □□ □□□ □ □□□□, □□□ □□ □ □□ □□ □□ □□□ □□□□. □□ □□□ □□ □□ □□□ □□ □ □, □□ □□ □ □□ □□□ □□□□ □□□□□□□.
□□ □□ □□□ □□□□ □□□ □□□□□ □□□□□?
A. □□ □□□□ □□ □□□ □□ □□□ □□□□□ □□□□□□□.
B. □□□ □□ □ □□□□ □□ □□□ □□□□□.
C. □□ □□ □ □□□□ □□□ □□□ □□□ □□□ □□□□□.
D. □□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□ □ □□□ □□□ □□□□ □□□ □.
Answer: C (LEAVE A REPLY)
opened
Explanation:
According to the ACAMS Study Guide 6th Edition, Chapter 2, page 37, one of the red flags of money laundering or terrorist financing is the use of nominees, trusts, or third parties to hide the

identity, ownership, or control of the funds or assets involved in the transaction. Nominees are individuals or entities that act on behalf of the actual or beneficial owners of a company, trust, or account, and may be used to conceal the source, destination, or purpose of the funds or assets. Nominees may also be used to evade taxes, sanctions, or regulatory requirements.
In this case, the compliance officer is unable to verify the identity of the beneficial owners of the company, and only information on the nominee owners was provided. This raises the suspicion that the company may be involved in money laundering or terrorist financing activities, and that the nominee owners may be acting as fronts or intermediaries for the actual or beneficial owners. The compliance officer should conduct further due diligence on the company, the nominee owners, and the beneficial owners, and report any suspicious or unusual activity to the relevant authorities.
Reference:
ACAMS Study Guide 6th Edition, Chapter 2, page 37
Beneficial Ownership Meaning and Regulation - Investopedia
What is a nominee shareholder? | LawBite

NEW QUESTION: 204
□□ □□ □□□ □□ □□□ □□ □□□ □□□□□ □□□ AML □□□□□ □□ □ □□□□ □□□□ □□□ □□□□□□. □□ □□ □□□ □□□ □□□? (2□□ □□□□□.)
A. □□ □□
B. □□ □□ □□
C. □□ □□□□ □□
D. □□ □□
E. □□□ □□□ □□
Answer: B,D (LEAVE A REPLY)
A deferred prosecution agreement (DPA) is a type of enforcement action that allows a financial institution to avoid criminal prosecution if it admits to wrongdoing, pays a fine, and agrees to remediate its AML program deficiencies within a specified period of time1. A cease and desist order (C&D) is another type of enforcement action that requires a financial institution to stop engaging in unsafe or unsound practices or violations of law, and to take corrective actions to address its AML program weaknesses2. Both of these actions are commonly used by regulators to address serious or systemic AML program failures by financial institutions, as evidenced by recent cases345.
Reference:
1: Deferred Prosecution Agreement - Wikipedia
2: FFIEC BSA/AML Appendices - Appendix R - Enforcement Guidance
3: FinCEN Announces $15 Million Civil Money Penalty against Bancrédito International Bank for Willful Violations of the Bank Secrecy Act
4: Lessons From The Seven Largest AML Bank Fines In 2021
5: Fines for AML Compliance Failures - ACAMS Today

NEW QUESTION: 205

□□ □□ □□ □□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □□□?

A. □□ □□□□ AML □□ □□□ □□□□ □□□.

B. □□□□□ □□□ □□ □□ □□□ □□□□ □□□.

C. AML □□□□□ □□ □□□□ □□□ □□□ □□□ □□□.

D. □□□ □□□□□ □□□ □□ □□ □□ □□□ □□□□ □□ □□□.

Answer: A (LEAVE A REPLY)

The line of business is responsible for creating, implementing and maintaining policies and procedures, as well as communicating these to all personnel. It must also establish processes for screening employees to ensure high ethical and professional standards and deliver appropriate training on AML policies and procedures based on roles and functions performed so employees aware of their responsibilities. To facilitate this, employees should be trained as soon as possible after being hired, with refresher training as appropriate.

NEW QUESTION: 206

□□□□□□□ □□ □□□ □□□□ □□□□□?

A. □□ □□□

B. FATF

C. □□□□□□ □□

D. □□□□ □□

Answer: (SHOW ANSWER)

Reference:

Basel Committee on Banking Supervision (Basel Committee) The Basel Committee was established by the G-10's central bank of governors in 1974 to promote sound supervisory standards worldwide. Its secretariat is appointed by the Bank for International Settlements in Basel, Switzerland.

NEW QUESTION: 207

□ □□ □□ □□□□ □□ □ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□□.

A. □□□

B. □□□□

C. □□□□

D. □□□□□□□□

Answer: D (LEAVE A REPLY)

A Mutual Legal Assistance Treaty (MLAT) is a formal agreement between nations allowing law enforcement cooperation in criminal investigations.

Option D (Correct): MLATs allow authorities to exchange information, request evidence, and collaborate on AML enforcement.

Option A (Incorrect): A Memorandum of Agreement (MOA) is a non-binding document for cooperation, not a legal treaty.

Option B (Incorrect): A Declaration of Understanding is informal and does not carry legal obligations.
Option C (Incorrect): MOUs are non-binding agreements, while MLATs create legal obligations.

NEW QUESTION: 208
□□□ □□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□ □□□□□□ □□ AML □□□ □ □□ □□□□□. □□□ □□□ □□□□ □ □□□ □□□□. □□□□ □□□ □ □□ □□□ □□□□□?
A. □□□ □□□□□ □□
B. □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□ □□□ □□
C. □□□□ □□□ □□ □□□ □□
D. □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□ □□□□ □□□ □□□□□.
Answer: A ([LEAVE A REPLY](#))
According to the Anti-Money Laundering Specialist (the 6th edition) study guide, one of the best practices for hiring an AML officer is to do a thorough background check, including verifying the candidate's credentials, qualifications, references, and reputation1. This is because the AML officer plays a crucial role in ensuring the compliance and integrity of the financial institution, and therefore must have the necessary skills, knowledge, experience, and ethics to perform the job effectively and professionally. A background check can also help to identify any potential conflicts of interest, criminal records, or regulatory sanctions that may affect the candidate's suitability for the position1. The other options are incorrect because:
B . Confering with the regulatory agency may not be necessary or appropriate, as the hiring decision is ultimately the responsibility of the financial institution, and the regulatory agency may not have any specific or relevant information or guidance on the candidate2.
C . Hiring the individual, relying on the recommendation of the correspondent, may not be sufficient or prudent, as the correspondent may have different standards, expectations, or interests than the financial institution, and may not have conducted a comprehensive or objective assessment of the candidate3.
D . Hiring the individual on a probationary basis may not be feasible or fair, as the AML officer role requires a high level of trust, authority, and responsibility, and the financial institution may not be able to evaluate the candidate's performance or potential in a short period of time4.
Reference:
1: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 147
2: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 148
3: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 147
4: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 148

NEW QUESTION: 209
□□ □□□□ □□ □□ □□ □□□□ □□□□□ □□□ □□□ □□□□□. □□ □□ □□ □ □ □□□ □□ □□□ □□□□□□.
□□□□□□ □□ □□□ □□□ □□□?

A. □□ □□□ □□□□ □□ □□ □□□□ □□
B. □□□ □□□□ □□ □□ □ □□ □□ □ □□
C. □□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□
D. □□□□ □□□ □□□ □□□ □□□ □□□□□ □□□ □ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
as there's NO mitigating control, the temporary control system must be developed and implemented until the permanent mitigating control is developed and implemented.

NEW QUESTION: 210
□ □□ □□□ □□ □□(FI)□ □□ □□□ □□□□ □□□ □□□□ □□□□□ □□□□ □□ □□ □□□ □□□□□□. FI□ □□ □□□ □□□ □□□□□?
A. □□□ □□□ □□ □□ □□□ □□□ □□□□□.
B. □□ □□□ □ □□ □□ □□□□ □□□ □□□ □□□□□.
C. □□□ □□□□ □□ □□□ □□□ □ □□ □□□ □□□ □□□□□.
D. □□□□□□ □□ □□□ □□□ □□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
Financial institutions (FIs) are required to cooperate with law enforcement agencies (LEAs) in their investigations of money laundering, terrorist financing, and other financial crimes. However, sometimes LEAs may submit requests for information or documents that are overly broad, unduly intrusive, or unreasonable in scope or volume. Such requests may pose challenges or risks for FIs, such as violating customer privacy, compromising data security, disrupting business operations, or incurring excessive costs.
The most appropriate response for an FI in such a situation is to narrow the request through a prompt response to the LEA. This means that the FI should communicate with the LEA as soon as possible to clarify the purpose, scope, and relevance of the request, and to negotiate a more reasonable and proportionate request that meets the LEA's needs and the FI's capabilities. The FI should also explain the potential difficulties or consequences of complying with the original request, and propose alternative or additional sources of information that may be more useful or accessible. The FI should document the communication and the agreed terms of the request, and comply with the request in a timely and accurate manner.
By narrowing the request through a prompt response, the FI can demonstrate its good faith and willingness to cooperate with the LEA, while also protecting its own interests and obligations. This can help avoid or resolve any conflicts or misunderstandings between the FI and the LEA, and facilitate a more efficient and effective investigation.
Reference:
Requests by Law Enforcement for Financial Institutions to Maintain Accounts EFFECTIVE SUPERVISION AND ENFORCEMENT BY AML/CFT SUPERVISORS OF THE FINANCIAL SECTOR AND LAW ENFORCEMENT Bank Secrecy Act/Anti-Money Laundering: Requests by Law Enforcement for Financial Institutions to Maintain Accounts Support of Law Enforcement ACAMS CAMS Certification Study Guide 6th Edition

NEW QUESTION: 211

□□ □□□□□ □□ □□(FI)□ ML/TF □□ □□□ □□□□□□□ □□□? (2□□ □□□□□.)

A. □□□ □□, □□□ □□ □□ □□□ □□□□ □□

B. □□ □□ □□ □

C. AML □□□□□□□□ □□□□□□ □□□□ □□

D. □□□ □□□□□□ □□□ □□

E. □□ □□□ □□□ □□□ □□□□ □ □

Answer: A,D (LEAVE A REPLY)

According to the ACAMS CAMS Certification Study Guide (6th edition), a financial institution (FI) should update its ML/TF risk assessment when there are changes in its business activities, customer base, or operating environment that may affect its exposure to ML/TF risks1 Some examples of such changes are:

When new products, services or customer types are introduced: New products, services or customer types may introduce new or increased ML/TF risks that the FI may not have previously considered or addressed. For example, offering online banking, prepaid cards, or cross-border remittances may create new opportunities for money launderers or terrorist financiers to exploit the FI's systems and processes. Therefore, the FI should assess the ML/TF risks associated with the new products, services or customer types and implement appropriate controls to mitigate them12 When the institution faces a merger or acquisition: A merger or acquisition may result in the FI inheriting the ML/TF risks of the other entity, as well as the potential liabilities and reputational damage that may arise from any ML/TF issues or violations. Therefore, the FI should conduct a due diligence on the other entity's ML/TF risk assessment, policies, procedures, and controls, and identify any gaps or weaknesses that need to be addressed. The FI should also integrate and harmonize the ML/TF risk assessment and compliance programs of the merged or acquired entity with its own13

NEW QUESTION: 212

□□□□□□□ □□□□□ □□□□ □□ □□□□□□ □□□ □ □□□ □□□□ □□□?

A. □□ □□

B. □□□□□□□□

C. □□

D. □□□ □□ □□

Answer: (SHOW ANSWER)

An anti-money laundering officer should coordinate with the human resources department when implementing a new hire screening program. A new hire screening program is a process of conducting background checks and verifying the identity, qualifications, and suitability of prospective employees, especially those who will be involved in the bank's anti-money laundering (AML) compliance program. The human resources department is responsible for managing the recruitment, hiring, and training of employees, and ensuring that they comply with the bank's policies and procedures. Therefore, the human resources department is the most appropriate partner for the anti-money laundering officer in developing and executing a new hire screening program that meets the bank's AML standards and regulatory requirements.

The other options are not relevant or necessary for the implementation of a new hire screening program. The internal auditor is responsible for evaluating the effectiveness and adequacy of the bank's internal controls, including the AML compliance program, but not for screening new hires. The local financial intelligence unit is a government agency that collects, analyzes, and disseminates financial information related to money laundering and terrorist financing, but not for screening new hires. The institution's regulator is the authority that supervises and examines the bank's compliance with the applicable laws and regulations, including the AML requirements, but not for screening new hires.

Reference:

ACAMS Study Guide for the CAMS Certification Examination (6th Edition), Chapter 4: Developing an AML/CFT Program 1 FFIEC BSA/AML Manual, Assessing the BSA/AML Compliance Program, BSA/AML Training 2 AUSTRAC, Employee due diligence 3

NEW QUESTION: 213

□□□ □□ □□□ □□□ □ □□ □□ □□□ □□□□□? (3□□ □□□□□.)

A. □□ □□

B. □□□ □□

C. □□ □□

D. □□ □□

E. □□ □□

F. □□ □□

Answer: (SHOW ANSWER)

When assessing the risk rating of customers, financial institutions should consider various factors that may indicate the potential for money laundering, terrorist financing, or other illicit activities. According to the ACAMS Study Guide for the CAMS Certification Examination1, some of the key risk factors are:

Customer risk: This refers to the characteristics of the customer that may affect their risk profile, such as their identity, occupation, source of funds, business activities, reputation, and political exposure. For example, customers who are politically exposed persons (PEPs), cash-intensive businesses, non-resident customers, or customers with complex ownership structures may pose a higher risk of money laundering or terrorist financing.

Geographic risk: This refers to the location of the customer, their business, or their transactions, and the level of risk associated with that location. For example, customers who are based in, operate in, or transact with jurisdictions that have weak anti-money laundering (AML) regulations, high levels of corruption, or are subject to sanctions or embargoes may pose a higher risk of money laundering or terrorist financing.
Product risk: This refers to the type of products or services that the customer uses or offers, and the level of risk associated with those products or services. For example, customers who use or offer products or services that are anonymous, complex, or facilitate cross-border transactions may pose a higher risk of money laundering or terrorist financing.
Other risk factors that may be considered include transaction risk, delivery channel risk, and industry risk2. However, these are not among the options given in the question.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, Chapter 4, Section 4.1, pages 97-99: "Customer Risk Factors", "Geographic Risk Factors", "Product Risk Factors".
Customer Risk Rating: Connecting Customer Risk Rating With Due Diligence, Section "Customer Risk Rating Factors": "Transaction Risk Factors", "Delivery Channel Risk Factors", "Industry Risk Factors".

NEW QUESTION: 214
Financial Action Task Force 40 Recommendations□ □□□ □□□ □□□ □□ □ □□□ □□ □ □□□□.
A. □□ □□□.
B. □□ □□□ □□.
C. □□□ □□□.
D. □□□ □□□□.
Answer: D (LEAVE A REPLY)
These designated nonfinancial businesses and professions (DNFBPs) include - casinos when customers engage in financial transactions equal to or above a designated threshold.......... - real estate agents when they are involved in transactions for clients concerning buying and selling properties; - dealers in precious metals and stones when they engage in any cash transaction with a customer at or above a designated threshold; - lawyers, notaries and independent legal professionals and accountants when they prepare or carry out transactions for clients concerning buying and selling real estate; ....; and - trust and company service providers when they prepare or carry out transactions for a client concerning certain activities ....

NEW QUESTION: 215
□□ □□□ AML □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□.
A. □□ □ AML □□ □□ □□□ □□□□□□□□.
B. AML □□□ □□ □□ □□□ □□ □□ □ □□□ □□□ □□ □□□□□ □□□□□ □□□ □□.
C. □□ □□□□ AML □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.

D. □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□ AML □□□ □□□□□.

Answer: D (LEAVE A REPLY)

According to the Anti-Money Laundering Specialist (the 6th edition) resources, one of the essential elements of an effective AML program is the establishment of a written AML policy that sets out the bank's commitment to comply with the applicable AML laws and regulations, as well as the roles and responsibilities of the board of directors, senior management, and staff in implementing the AML program. The AML policy should also include the bank's risk assessment, customer due diligence, transaction monitoring, record keeping, reporting, training, and audit procedures. The AML policy should be approved by the board of directors and communicated to all staff from the top down. The other options are not incorrect, but they are not the primary responsibility of the board of directors in demonstrating commitment to AML compliance.

Reference:

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 8: Anti-Money Laundering Programs, page 221.

: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 8: Anti-Money Laundering Programs, page 224.

NEW QUESTION: 216

□□ □□ □□ □□□(Basel Committee on Banking Supervision)□ 2001□ 10□□ □□□ □□ □□ □□ □□(Know Your Customer) □□□□□□ □□□ □□ □□□ □□ □□□ □□□□□ □.

A. □□ □□ □□□.

B. □□ □□ □□.

C. □□ □□□ □□.

D. □□ □□ □□.

Answer: C (LEAVE A REPLY)

The Basel Committee on Banking Supervision (BCBS) issued a paper in October 2001 titled Customer due diligence for banks, which outlined four essential elements of a sound Know Your Customer (KYC) programme. These elements are: customer acceptance policy, customer identification, on-going monitoring of higher risk accounts, and risk management. The paper also recommended that these standards should be applicable to all banks in all countries, regardless of their size, nature, or location. The paper stated that "KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities."1

Reference:

Customer due diligence for banks by the Basel Committee on Banking Supervision, October 2001.

Consolidated KYC Risk Management by the Basel Committee on Banking Supervision, October 2004.

Editorial The Basel Committee on Banking Supervision report on customer ... by Journal of Banking Regulation, 2002.

NEW QUESTION: 217

□□ □□ □□□□□ □□□□ □□□□ □□ □□□□□ □□□□□ □□ □□ □□□□ □□□□□ □□ □□ □□ □□□ □□□□□□□. □□ □□□□ □□□□ □□ □□□□ □□ □□ □□ □□ □□□□ □□□□ □ □ □□□□□ □□□□ □□□□ □□□□□□ □□ □□□(STR)□ □□□□□□□□.
□□□□□□□ □□ □□□□ □□□□ □□□□ □□□□ □□ □□□□□ STR □□□□ □□□□ □□□□□ □ □□?

A. □□□ □□ □□□□□ □□□□.
B. □□□□□□ STR □□□□□ □□
C. □□ □□□□ □□ □□□□ □□□□ □□□□□□ □□□□□.
D. □□□□□□□ □□□□□ □□□□□

Answer: B ([LEAVE A REPLY])

The best option for the compliance officer is to follow the financial institution's established STR reporting policy, which should include procedures for reporting suspicious activity involving senior management or board members. This would ensure that the compliance officer acts in accordance with the bank's internal controls and governance, and avoids any potential conflicts of interest or breaches of confidentiality. The other options are not advisable because they could either compromise the integrity of the STR filing, expose the compliance officer to legal or reputational risks, or alert the subject of the investigation.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 4, page 1401
ACAMS CAMS Certification Video Training Course, Module 4, Lesson 22 ACAMS CAMS Certification Practice Exam, Question 843

NEW QUESTION: 218

□□□□□ □□□□ □□ Wolfsberg □□□ □□□□ □□ □ 3□□□ □□□□□ □□□□ □□□□□ □□ □□□ □□□□ □□ □□□□ □□□□□□.

A. □□ □□
B. □□□□ □ □□ □□□□□ □□□□□ □□ □□□□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□
C. □□ □□□□ □□□□ □□□□ □□□□ □□□□□ □□ □□□□ □□□□ □□ □ □□□□ □□□□□ □□ □ □□□□ □□
D. □□□(□□□□ □□□□ □□□□ □□ □□ □□)

Answer: ([SHOW ANSWER])

The Wolfsberg Principles for Private Banking are a set of guidelines for private banking relationships that aim to prevent and detect money laundering and terrorist financing risks. The Principles state that the bank should conduct additional due diligence on clients and beneficial owners in certain circumstances that may indicate a higher risk of money laundering or terrorist

financing. Among the options given, A, B, and C are the correct choices that reflect the circumstances listed in the Principles.
Foreign jurisdictions are countries or territories other than the one where the bank operates or where the client or beneficial owner resides. The Principles state that the bank should conduct additional due diligence on clients and beneficial owners who are connected to foreign jurisdictions, especially those that have weak or inadequate anti-money laundering standards, or that are subject to sanctions, embargoes, or similar measures.
High Risk Countries are countries or territories that are identified by credible sources, such as the Financial Action Task Force (FATF), as having inadequate anti-money laundering standards, or as being a source, transit, or destination of illicit funds. The Principles state that the bank should conduct additional due diligence on clients and beneficial owners who are connected to high risk countries, and apply enhanced measures to mitigate the risks.
High Risk activities are activities that involve clients and beneficial owners whose source of wealth or funds originates from sectors or industries that are known to be vulnerable to money laundering, such as cash-intensive businesses, gambling, arms trade, precious metals and stones, or art and antiquities. The Principles state that the bank should conduct additional due diligence on clients and beneficial owners who are engaged in high risk activities, and verify the legitimacy and origin of their wealth and funds.

NEW QUESTION: 219
□□ □□□ □□□□ □□□ □□□ □□□□.
A. □□□ □□□ □□□□□.
B. □□□□□□ □□□ □□ □□□ □□ □□ □□□□□.
C. □□ □□□ □□□□□.
D. □□ □□ □□□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
Economic sanctions are penalties imposed by one or more countries against another country, group, or individual for violating international norms or threatening national interests1. The ultimate goal of economic sanctions is to protect national security by changing the behavior or policies of the target, or by weakening its capabilities or resources2. Sanctions can be used to advance various foreign policy objectives, such as counterterrorism, nonproliferation, democracy promotion, human rights protection, conflict resolution, and cybersecurity1. Sanctions can take different forms, such as travel bans, asset freezes, trade embargoes, arms restrictions, and aid reductions1. Sanctions can be applied unilaterally by one country, or multilaterally by a coalition of countries or an international organization, such as the United Nations or the European Union1.
Reference:
1: What Are Economic Sanctions? | Council on Foreign Relatio
2: How Economic Sanctions Work - Investopedia

NEW QUESTION: 220

MLRO(Money Laundering Reporting Officer)□ □□ □□□□ □□ □□□ AML □□□□□ □□ □ □□□ MLRO□ □□ □□□ □□□□□□□□. MLRO□ □□ □□□ □□ □□□ □□ □□□ □□□□□?

A. MLRO□ AML □□□□ □□□ □□ □□□ □ □ □□ □□□ □□□□□.

B. MLRO□ □□ □□ □□□ □□ AML □□□□ □□□ □□□□ □□□□ □□□ □□ □ □□ □□.

C. MLRO□ □□□ AML □□□□ □□□ □□ □□□ □□ □□□ □□ □□□ □□□□□□.

D. □□□ AML □□□□ □□□ □□ □□□ □ □ □□ □□□ MLRO□ □□ □□□ □□□□□ □.

Answer: (SHOW ANSWER)

MLROs are responsible for implementing and enforcing an appropriate risk-based approach for their firm, ensuring compliance with the relevant laws and regulations, and reporting any suspicious activities to the authorities. If they fail to discharge their duties, they may face personal liability and civil or criminal sanctions. MLROs are not the only individuals that can be held responsible for AML program deficiencies, as other senior managers, directors, or partners may also be liable depending on their role and involvement. However, MLROs are often the primary focus of enforcement actions due to their specific responsibilities and obligations. MLROs cannot avoid liability by agreeing to a civil penalty, as this does not absolve them from their legal duties or potential criminal prosecution. Banks can also be found liable for AML program deficiencies and face fines, penalties, or other sanctions.

Reference:

Technical factsheet The role of the money laundering reporting officer

Consequences of not complying | AUSTRAC

Money Laundering Reporting Officer: The Role Of MLRO

FinCEN Penalizes U.S. Bank Official for Corporate Anti-Money Laundering Failures

NEW QUESTION: 221

□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□.

A. □□□□ □□□ □□□ □□□□ □□ □ □□□□ □□□ □□□□ □□□ □□□□□.

B. □□□ □□(NGO)□ □□ □□□ □□ □□□ □ □□□ □□ □□□ □□□□ □□□□□.

C. □□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□□□.

D. □□ □□□ □□□ □□□□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□□ □□.

Answer: D (LEAVE A REPLY)

Economic sanctions are used as a non-military tool to enforce foreign policy and national security objectives.

Option D (Correct): Sanctions aim to change the behavior of entities engaged in money laundering, terrorist financing, or other illicit activities.

Option A (Incorrect): Sanctions do not necessarily indicate military action.

Option B (Incorrect): NGOs may be exempt from sanctions, but this is not their primary purpose.

Option C (Incorrect): While human rights concerns can lead to sanctions, they are primarily imposed to change behavior.

NEW QUESTION: 222
□□ □□□ □□□ □ □□□ □□□□ □□□ □ □□□□ □ □□□ □□□□□?
(2□□ □□□□□.)
A. □□ □□
B. □□□□
C. □□ □□
D. □□ □□
E. □□ □□
Answer: A,C (LEAVE A REPLY)
Customer composition and product offerings are two important factors that affect the level of risk exposure for a financial institution (FI) in terms of money laundering and terrorist financing. Customer composition refers to the types of customers that the FI serves, such as individuals, businesses, non-profit organizations, or politically exposed persons (PEPs). Different customer segments may pose different levels of risk depending on their activities, sources of funds, geographic locations, and connections to other entities. For example, customers that are cash-intensive, have complex ownership structures, operate in high-risk jurisdictions, or are associated with PEPs may present higher risk indicators than customers that are transparent, regulated, and operate in low-risk jurisdictions12. Product offerings refer to the types of products, services, and transactions that the FI provides, such as deposits, loans, wire transfers, trade finance, or digital assets. Different products, services, and transactions may have different levels of vulnerability to money laundering and terrorist financing depending on their features, complexity, volume, and speed. For example, products that are anonymous, involve high-value or cross-border transfers, enable rapid movement of funds, or involve new or emerging technologies may present higher risk indicators than products that are identifiable, involve low-value or domestic transfers, require multiple verification steps, or involve established or traditional technologies12.
Reference:
1: Risk Assessment: Risk Factors & Mitigating Measures2
2: Risk Assessment: Process, Examples, & Tools1

NEW QUESTION: 223
□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□ □□ □□
B. □□□ □□ □□□ □□
C. □□ □□
D. □□ □□□□ □□
Answer: A (LEAVE A REPLY)
free of payment asset transfer is a trading pattern that may be indicative of money laundering in capital markets. Free of payment asset transfer is a method of transferring securities without any

corresponding payment, which can be used to avoid detection of the origin or destination of the funds. This can facilitate the layering or integration stages of money laundering, as the launderer can move the assets across different accounts, jurisdictions, or institutions without leaving a clear audit trail. Free of payment asset transfer can also be used to evade taxes, sanctions, or other regulatory requirements.
Reference:
ACAMS Study Guide 6th Edition, Chapter 1, Section 1.8, page 28: "Methods to launder money using broker-dealers, investment advisors, and the capital markets (e.g., securities, futures)".
ExamTopics, Question 476: "Which trading pattern may be indicative of money laundering in capital markets?"

NEW QUESTION: 224
□□ □□□ □□ □□□□□ □□□ □□□□□ □□□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
□□ □□□ □□ Wolfsberg □□ □□ □□ □□□ □□□□□□ □□ □□□□ □□ □□□ □□ □ □□ □□□ □□□□□□ □□□? (2□□ □□□□□□.)
A. □□□□ □□□ □□□ □□□ □ □□□ □□□□ □□□ □□ □□□ □□□ □□□ □□□ □.
B. □□□□ □□□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□ □□□ □□□ □□□ □□□ □□□ □□ □□□ □□□.
C. □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□ □□ □□□□□□ □□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□□ □□ □□.
D. □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□□□ □□□ □□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□. □□ □□ □□□□□□ □□ □□.
Answer: B,C (LEAVE A REPLY)
According to the Wolfsberg Anti-Money Laundering Principles for Private Banking (2012), the bank should have a clear policy on how to deal with intermediaries, such as lawyers, accountants, trust and company service providers, or other financial institutions, that introduce or manage clients on behalf of the bank. The policy should reflect the following aspects1:
The bank should perform due diligence on the intermediary itself, including its ownership, reputation, regulatory status, and AML policies and procedures.
The bank should obtain the identity and beneficial ownership information of the clients introduced or managed by the intermediary, and verify them using reliable and independent sources, unless there are legal or regulatory impediments to do so.
The bank should assess the level of due diligence performed by the intermediary on its clients, and determine whether it is equivalent or comparable to the bank's own standards. If not, the bank should perform additional due diligence on the intermediary's clients, or decline to accept them.

The bank should monitor the transactions and activities of the clients introduced or managed by the intermediary, and report any suspicious or unusual activity to the relevant authorities.
Option B is consistent with these aspects, as it states that the bank must obtain the same type of information with respect to an introduced client that would otherwise be obtained by the bank, absent the involvement of the intermediary. This ensures that the bank has a sufficient understanding of the client's identity, source of wealth, and risk profile, and can apply appropriate AML measures.
Option C is also consistent with these aspects, as it states that where an intermediary manages assets on behalf of a number of clients and is the account holder with the bank, but that intermediary does not conduct the same level of due diligence as the bank, it is necessary for the bank to undertake due diligence on the intermediary's clients. This ensures that the bank does not rely solely on the intermediary's due diligence, and can identify and mitigate any potential money laundering risks associated with the clients.
Option A is not consistent with these aspects, as it states that when an intermediary introduces clients to the bank, it is not necessary for the bank to perform due diligence on the intermediary's clients. This contradicts the principle that the bank should obtain and verify the identity and beneficial ownership information of the clients introduced by the intermediary, unless there are legal or regulatory impediments to do so.
Option D is also not consistent with these aspects, as it states that where an intermediary manages assets on behalf of a number of clients and arranges for the opening of accounts for its clients with the bank, and that intermediary is a financial institution subject to similar regulations, it is necessary for the bank to perform due diligence on the intermediary's clients. This contradicts the principle that the bank may rely on the due diligence performed by the intermediary on its clients, if the intermediary is a regulated financial institution that applies equivalent or comparable AML standards to the bank, and if the bank has access to the relevant information and documentation.
Reference:
1: Wolfsberg Anti-Money Laundering Principles for Private Banking (2012), Section 3: Intermediaries

NEW QUESTION: 225
□□□ □□□ □□ □□ □□ □□□□ □□ □□□ □□□□ □□□ □□□ □□ □□□ □□□ □□□□ □□□□□ □□□ □□□□□□. □ □□□ □□□ □□ □□□□□ □□□ □□ 3□□ □□□ □□□□□ □□□ □□(□□□)□ □□□ □□□ □□□□□□. □□□(□□□)□ □□□ □□□ □□ □□□□□ □□□ □□ □□ □□□□ □□□□ □□□□□. □□ □□□ □□□ □ □□□□ □□□(□□□)□ 15□ □□ □□□ □ □□ □□□□ □ □□ □ □□ □□ □□□ □□ □ □□□ □□ □ □□ □□ □□ □□ □□□ □□□□□ □□□□□. □□□□ □□ □□□ □□ □□□□ □□ □□ □□ □□ □□□□□ □□ □□□ □□□ □□ □□□□□. □□□(□□)□ □□

A. □□□ □□ □□□□□□□.

B. □□□(□□)□ □□ □□□ □□□□□□ □□.

C. □□□(□□)□□ □□□□□□ □□ □□□ □□□ □□□□□□.
D. □□(□□)□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The specialist should recommend directing the teller (cashier) to file a suspicious transaction report (STR). This is because the teller (cashier) has failed to comply with the bank's internal policies and procedures for reporting unusual or suspicious activity, which is a key component of an effective anti-money laundering (AML) program1. The teller (cashier) should have filed an internal report of unusual activity as soon as he or she noticed the suspicious transactions, regardless of the personal circumstances or the length of service of the customer involved2. Failing to do so could expose the bank to regulatory sanctions, reputational damage, or legal liability3.
The other options are not appropriate recommendations for the specialist to make in this situation. Continuing to monitor the accounts is not sufficient, as it does not address the past non-compliance or the potential money laundering risk posed by the suspicious transactions. Refreshing anti-money laundering training for the teller (cashier) is not enough, as it does not ensure that the teller (cashier) will report the suspicious transactions or prevent future violations. Suspending the teller's (cashier's) employment is too harsh, as it does not take into account the teller's (cashier's) long and exemplary work record, the personal hardship faced by the teller's (cashier's) family, or the possibility of remedial actions or corrective measures4.
Reference:
1: Internal Controls | FinCEN.gov1 2: Reporting Suspicious Transactions - ACAMS2 3: The Consequences of Non-Compliance with AML Regulations - Blog | Unit213 4: Employee Discipline in the Workplace: A Guide for Managers4

NEW QUESTION: 226
□□ □ □□□□□□□ □□□□□ □□□□□ □□ □□□□□□ □□□ □ □□□□□ □□ □□?
A. □□□□□□
B. □□□□□□□□
C. □□□□□
D. □□□ □□ □□
Answer: C (LEAVE A REPLY)
An anti-money laundering officer should coordinate with human resources when implementing a new hire screening program, because human resources is responsible for managing the recruitment, hiring, and training of employees, as well as ensuring compliance with labor laws and regulations. A new hire screening program is a key component of an effective anti-money laundering (AML) program, as it helps to prevent the hiring of individuals who may pose a risk of facilitating money laundering, terrorist financing, or other financial crimes, or who may have a criminal or disciplinary history that could compromise the integrity of the institution. A new hire screening program should include background checks, verification of credentials and references, and assessment of skills and competencies relevant to the AML function. An anti-money laundering officer should work closely with human resources to establish the criteria, procedures,

and documentation for the screening program, as well as to monitor its implementation and effectiveness.
Reference:
ACAMS CAMS Certification Video Training Course1, Module 4: Developing an AML Program, Lesson 4.2: Developing an AML Program ACAMS CAMS Study Guide, 6th Edition2, Chapter 4: Developing an AML Program, Section 4.2: Developing an AML Program, pp. 81-82 ACAMS CAMS Examination Preparation Seminar, 6th Edition3, Chapter 4: Developing an AML Program, Section 4.2: Developing an AML Program, Slide 20

NEW QUESTION: 227
□□ □ □□□□□ □□□ □□□ □□□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□□□ □□□□□ □□□ □□ □□□□□.
B. □□□□□ □□□□□ □□ □□□ □□□□□□□.
C. □□ □□□ □□□□□ □ □□□ □□□ □□□ □□□□□.
D. □□□ □□ □□□ □□□□□ □□□□□ □□ □□□□□ □□□□.
Answer: D (LEAVE A REPLY)
One of the common methods used by money launderers to hide the origin and destination of illicit funds is to create complex corporate structures that obscure the identity of the real owners or controllers of the assets. Lawyers can facilitate this process by providing legal services such as setting up shell companies, trusts, foundations, or other entities in jurisdictions with weak AML regulations or high secrecy. By doing so, lawyers can help their clients evade taxes, avoid sanctions, conceal criminal activities, or launder money. This is why lawyers are considered high-risk professionals for AML purposes and are subject to due diligence and reporting obligations.
Reference:
ACAMS Study Guide for the CAMS Certification Examination, Chapter 3, Section 3.2.2, page 77: "Lawyers are often used to create complex corporate structures that can be used to hide the beneficial ownership of assets." Money Laundering Reporting Officer: The Role Of MLRO, Section "Money Laundering Risks For Lawyers": "Lawyers are at risk of being used by criminals to launder money through various means, such as creating corporate entities, conducting transactions, or providing advice." New York Lawyer Pleads Guilty to Ponzi Scheme, Money Laundering, Section "Lawyer agrees to forfeit $19 million from investment scheme": "A New York lawyer admitted Monday to money laundering and orchestrating an $18.8 million Ponzi scheme using his Forest Hills-based law firms, Wisnicki & Associates LLP and Wisnicki Neuhauser LLP."

NEW QUESTION: 228

□□ □□ □□ □□ □□ □□□ □□□□□□ □□□□ □□ □□□□□□?

A. □□□□

B. □□□□

C. □□

D. □□□

Answer: D (LEAVE A REPLY)

Structuring is the intentional evasion of a reporting or recordkeeping requirement by breaking down a large transaction into smaller ones, or by using multiple accounts, institutions, or persons to avoid triggering the threshold for reporting or recordkeeping. Structuring is also known as smurfing, and it is a common technique used by money launderers to conceal the source, ownership, or control of illicit funds.

Reference:

ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 2, Section 2.1.1, page 511 ACAMS CAMS Certification Video Training Course, Module 2, Lesson 2.1, video time 7:00-8:002 ACAMS CAMS Certification Practice Exam, Question 134, page 2853

NEW QUESTION: 229

□□ □□□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □ □□□□□□ □□□□ □□ □□ □□□ □□□□□□?

A. □□□ □□ □□ □□□□ □□ □□□ □□ □□□ □□

B. □□□□ □□□

C. □□□□ □□ □□□ □□

D. □□ □□□□ □□□□ □□ □□ □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 230

USA PATRIOT Act□ □□ □□□ □□ □□□ □□□ □ □□ □□(FI)□ □□ □□ □□□ □□□ □□□ □□□□□?

A. □□ FI□ □□ □□ □□□□ □□ □ □□□ □□□□□.

B. □□□ □□□□ □□ FI□ □□□ □□.

C. □□ □ □□□ □□ □□□ □□□□□ □□ □□□□□ □□□□□.

D. □□ □□ □□ □□□ □□□ □□□ □□ □ □□□ □□ □□□ □□ □□□ FI□ □□□□□ □□□□□.

Answer: (SHOW ANSWER)

According to the CAMS manual 6th edition, the USA PATRIOT Act allows the US government to subpoena documents from foreign financial institutions (FIs) that have no presence in the US (option B). The manual states that "The USA PATRIOT Act provides US law enforcement agencies with the power to subpoena documents from foreign banks that maintain correspondent accounts with US banks or have no presence in the United States" (p. 77).

NEW QUESTION: 231

□□ □□ □□□ □□(FATF)□ □□ □□□ □□ □□ □□/□□□□ □□□ □□ □□ □□□ □ □□ □□□ □□□ □ □□ □ □□ □□ □□ □□□ □□□ □ □□ □□□□□?

A. □□ □□ □□□ □□ □□ □□

B. □□ □□ □□□ □□□ □□□□□ □□

C. □□ □□ □□□□□ □□ □□

D. FATF□ □□ □□□ □□ □□□ □□□□ □□

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

The FATF is an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures to combat money laundering, terrorist financing and other related threats to the integrity of the international financial system1. The FATF identifies jurisdictions with serious strategic deficiencies in their anti-money laundering / counter financing of terrorism (AML/CFT) regimes and issues public statements to warn the international community of the risks emanating from these jurisdictions2. These jurisdictions are also known as high-risk jurisdictions subject to a call for action, or the "black list" in external sources2. The FATF urges its members and all other jurisdictions to apply counter-measures to protect themselves from the money laundering and terrorist financing risks posed by these jurisdictions2. Counter-measures are enhanced due diligence or restrictive measures that go beyond the normal AML/CFT requirements, such as requiring additional information or documentation, rejecting transactions, restricting business relationships, or terminating correspondent banking relationships3. The FATF also provides guidance on the types and levels of counter-measures that may be appropriate, depending on the specific risks and circumstances of each jurisdiction3.

Reference:

1: What is the FATF? | FATF

2: High-Risk Jurisdictions subject to a Call for Action | FATF

3: Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction | FATF

NEW QUESTION: 232

□ □□□□□□ □□□□ □□ □□ □□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□ □□□□□□. □□ □□ □□□□ □□□□□ □□□ □ □□ □□ □□ □□□ □□□□□?

A. □□ □□

B. □□□ □□

C. □□□

D. □□ □□□

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

According to the Anti-Money Laundering Specialist (the 6th edition) study guide, structuring is a technique used by money launderers to avoid triggering currency transaction reporting requirements by breaking down large amounts of cash into smaller deposits that are below the reporting threshold1. Structuring can also involve withdrawing cash in small amounts from different locations or branches to evade detection and scrutiny2. Therefore, the compliance analyst is potentially identifying structuring as the type of money laundering in this case.
Reference:
1: CAMS Study Guide, 6th Edition, Chapter 1, Section 1.3, page 14
2: CAMS Study Guide, 6th Edition, Chapter 1, Section 1.4, page 15

NEW QUESTION: 233
□□□□□□□(OFAC)□ □□ □□ □□□ □□□□ □□□ □□□ □ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□ □□ OFAC □□ □□□ □□□ □□
B. □□□ □□□ □□ □□□ □□□□ □□□ □□□□ □□ OFAC □□□□ □□□□□ □□
C. □□□ □□□□ □□ □□ □□ □□ □□□ OFAC □□□ □□□□ □□□□
D. □□ □□ □□□ □□□□ □□□ □□ OFAC □□ □□□□□ □□ □
Answer: (SHOW ANSWER)
The Office of Foreign Assets Control (OFAC) administers and enforces economic sanctions programs [1][2], which are designed to protect US national security, foreign policy, and economic interests. Transactions that would otherwise be prohibited can be allowed through an OFAC licensing process, in which the OFAC evaluates the request to determine that the transaction does not undermine US policy objectives.

NEW QUESTION: 234
□□□□ □□□ □□ □□ □□□□□□ □□□□□ □□□□□ □□□ □□□□□ □□□□ □
□□ □□□ □□□□ □□□ □□□□. □□□□ □□□□□□□ □□□ □□□□.
□□□□□□ □□□ □□□ □ □□ □□□ □□□ □□□?
A. □□□ □□□ □□ □□□ □□
B. □□□□ □□□□ □□□ □□□□
C. □□□ □□ □□□□ □□□ □□□ □□□□.
D. □□□□□ □□□ □□□□□ □□□ □□□ □□□.
Answer: C (LEAVE A REPLY)
The compliance officer should inform the bank's legal counsel and follow their instructions when informed of the regulator's notice. This is the most prudent and professional course of action, as it ensures that the compliance officer acts in accordance with the bank's policies and procedures, as well as the applicable laws and regulations. The compliance officer should also document the communication and cooperation with the legal counsel and the regulator, and preserve all relevant records and evidence relating to the matter. The compliance officer should not take any action that could compromise the integrity or confidentiality of the investigation, such as destroying records, insisting on the president's resignation, or informing the president of the suspicions.

Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, page 47
ACAMS CAMS Certification Exam Outline, 6th Edition, Domain 2, Task 2.4
ACAMS CAMS Certification Video Training Course, Module 2, Lesson 2.4
Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition), Question 337

NEW QUESTION: 235
□□□ □□□ □□□ □□□□ □□□ 25□ □□ □□□□ □□□□□□. □□□□□ □□ □□ □□□ □□ □□□ □□ □□□□ 1,500□□□ □□□□ □□□□□□. □□ □□□□ □ □□□ □□ □□ □□ □□□ □□□□□. □□ 4□□ □□ □□ □□ □□□, □□□, □□□□ □□□ □□□□ □□ □□□ 3,000□□□ □□□ □□□□□□. □□ □□□ □□□ □□ □□ □□□□ □□□ 8,500□□ □□□ □□ □□□ □□□□ □□□ □□□□□□. □□□ □□□□□□(STR) □ □□□□□ □□.
STR□ □□□□□ □ □□□ □□□ □□□□□?
A. □□ □□□ □□□ □□ □□
B. □□□ □□ □□ □ □ □□□ □□
C. □□□□ □□□□□ □ □□ □□□ □□
D. □□□ □□ □□□ □□□□ 25□ □□ □ □□□ □□□□□ □□
Answer: (SHOW ANSWER)
The important fact to include in the STR is the recent change in the timing of deposits and withdrawals in the account, as this indicates a possible change in the customer's source and use of funds, and may suggest money laundering or other illicit activity. The customer's work history, the amount of his monthly retirement check, the fact that he is well known to the bank staff, and the fact that he has lived in the area and banked at this bank for 25 years are not relevant for the STR, as they do not explain the unusual pattern of transactions in his account.
Reference:
CAMS Certification Package - 6th Edition | ACAMS, Chapter 4: Conducting and Supporting the Investigation Process, page 131 CAMS Certifications: How to Get CAMS Certified | ACAMS, CAMS Examination Preparation, page 8 ACAMS CAMS Certification Video Training Course - Exam-Labs, Video 4.2: Suspicious Transaction Reporting Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition), Question 97

NEW QUESTION: 236
□□□ □□□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□□□. □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□□□ □□ □ □□ □□□ □□□ □□□?
A. □□ □□□□ □□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□□□□□□ □□□ □□ □□□ □□□□.
D. □□□□ □□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)

According to the FATF Recommendations, financial institutions should maintain all necessary records on transactions and customers for at least five years, and make them available to competent authorities upon appropriate authority1. This includes records and documents related to suspicious transactions that have been reported to the financial intelligence unit (FIU) or other designated authorities. Providing the supporting documentation to competent authorities upon request is essential for the investigation and prosecution of money laundering and terrorist financing offences, as well as for the identification and tracing of criminal assets2.
Hinting to the customer that she should come in and explain her behavior is not a correct answer, as it may tip off the customer about the suspicion and compromise the effectiveness of the reporting system. Financial institutions should not disclose to the customer or to third parties that a suspicious transaction report (STR) or related information is being reported to the FIU3.
Maintaining adequate written documentation of all individuals and transactions reported is not a sufficient answer, as it does not imply cooperation with competent authorities. Financial institutions should not only keep records, but also provide them to the authorities when requested.
Submitting information upon receiving a legal request from parties involved in a civil lawsuit is not a relevant answer, as it does not relate to the cooperation with competent authorities for AML/CFT purposes. Civil lawsuits are not part of the AML/CFT framework, and financial institutions should not disclose confidential information to private parties without proper legal grounds.
Reference:
FATF Recommendation 11: Record-keeping 1
FATF Recommendation 31: Powers of law enforcement and investigative authorities 2 FATF Recommendation 21: Tipping-off and confidentiality 3

NEW QUESTION: 237
□□□□□□ □ □□□ □□□ □□ □ □□ □□□ □□ □□□ □□□□□□ □ □□□ □□□ □□ □ □□□ □□□□□□. □ □□ □□ □□ □□□ □□□□□ □□□□.
□□□□□ □□□ □□□ □□□ □□□□□ □□□ □□□□□ □□ □□□□□ □ □□ □□□ □□□ □□□□□□?
A. □□□ □□ □□□ □□ □□□ □□□□□ □□ □□□□□ □□□ □□ □□ □□□ □□ □□□ □□□ □ □□□□□.
B. □□□□□ □□□ □□□□□ □□□ □□ □□□ □□□□□, □□□ □□□ □□□□□ □□ □□□ □ □□□ □□□□□□□ □□□ □□□ □□□.
C. □□ □□□ □□ □□□ □ □□□□□ EU□ □□□ □□ □ □□□□□ □□ □□□□□ □ □□□ □□.
D. □□□□□ □□□ □□ □□□ □□ □ □□□ □□ □□□□□ □□□□□□ □□□□□ □□□ □□ □□□ □□□□□ □□□.
Answer: D (LEAVE A REPLY)
Banks within the EU must comply with AML laws and data privacy regulations before sharing customer data.

Option D (Correct): Information sharing should be limited to what is necessary and proportionate, following GDPR and AMLD regulations.
Option A (Incorrect): AML laws allow information-sharing in certain cross-border investigations.
Option B (Incorrect): While legal review is necessary, a production order is not always required for AML-related information sharing.
Option C (Incorrect): Data protection laws (e.g., GDPR) must still be respected, even in financial crime investigations.

NEW QUESTION: 238
Financial Action Task Force□ □□□ □□ □□□ □□□ □□□□ □□□.
A. □□□ □ □□□ □□□ □□□ □□□□ □□ □□ □□.
B. □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ AML □□□□□□□.
C. AML □ □□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□ □□□□□.
D. AML □□□ □□ □□ □ □□□ □□□ □□ □□□ □□□□.
Answer: (SHOW ANSWER)
According to the web sources I found, FATF Recommendation 18 requires financial institutions to implement group-wide programmes against money laundering and terrorist financing that include policies and procedures for sharing information within the group for AML/CFT purposes12. These programmes should also include compliance management arrangements, screening procedures for hiring employees, an independent audit function and ongoing employee training1.

NEW QUESTION: 239
□□ □□ □□□ □□ □□ □□□ □□□ □ □□ □□□ □□□□ □□□ □□□□□ □□ □□ □□□ □□ □□□ _______□□ □□□?
A. □□□ □□□□ □□ □□□□ □□ □□□ □□□□□. □□□ □□□ □□□ □□ □□□ □ □ □□ □□□□□ □□□□ □□□.
B. □□□ □□ □□□ □□ □□ □□□ □□□ □□ □□□ □ □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□□ □□ □□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□□. □□□ □□ □□□ □ □□ □□□□ □□□ □□□□□ □□ □ □□□□.
D. □□ □□ □□□ □□ □ □□□ □□□□ □□: □□□-□□□□□ □□ □/□□ □□-□□. □ □□ □□□ □ □□□ □□□ □□□□.
Answer: (SHOW ANSWER)
According to the Anti-Money Laundering Specialist (the 6th edition) study guide, one of the best practices for conducting an internal investigation is to request formal company authorization to conduct the investigation. Such authorization should be granted, if possible, by the board of directors or audit committee, as this will help to establish the independence and legitimacy of the investigation, as well as the protection of the attorney-client privilege and the work product doctrine1. The other options are incorrect because:

B . Refusing to provide any records or documents to law enforcement may be seen as obstructing justice or violating regulatory obligations, and may also result in the loss of the privilege or the imposition of sanctions or penalties23.
C . Letting the bank hire any and all contract investigators may compromise the quality and integrity of the investigation, as well as the protection of the privilege or the work product doctrine, as the investigators may not be properly supervised or instructed by legal counsel, or may not be covered by the Kovel doctrine45.
D . Not marking files or documents with privileged and confidential: attorney-client privilege and/or work-product may undermine the claim of the privilege or the work product doctrine, as it may indicate that the materials were not prepared for the purpose of seeking or providing legal advice or in anticipation of litigation, or that they were not intended to be kept confidential67.
Reference:
1: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 150
2: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 151
3: Perkins Coie, Protecting Internal Investigation Materials From Disclosure, Updates, August 10, 2020
4: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 150
5: Eversheds Sutherland, Legal privilege of corporate internal investigations under US law - 2019 caselaw update, JDSupra, December 20, 2019
6: ACAMS, CAMS Certification Package - 6th Edition, Chapter 5, page 150
7: Norton Rose Fulbright, Internal investigations: when does privilege apply?, Global law firm, September 11, 2018

NEW QUESTION: 240
□ □□□□□ □□□ □□ □□□ □□□□□ □□□□□□? (2□ □□).
A. □□□ □□□ □□□□□ □□□ □□□ □□□ □ □□ □□□□□ □□□□□ □□□□.
B. □□ □□□ □□□ □□□□□ □□□ □□ □□□ □ □□ □□□ □ □□ □□□□□□.
C. □□□□□□ □□ □ □□ □□ □□□ □□□□□□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□.
D. □□□ □□□ □□□□□□ □□□□□ □□□□□ □□ □□□ □□□□□ □□□ □□ □□□ □ □ □□□.
E. □□□ □□ □□□ □□□□□ □□ □□□□□ □□□ □□□ □ □□ □□□□□□.
Answer: (SHOW ANSWER)
Organized crime groups often use front companies to disguise the origin and destination of their illicit funds, and to integrate them into the legitimate economy. Front companies are businesses that appear to be engaged in lawful activities, but are actually controlled by criminals for money laundering purposes.
One reason why organized crime groups use front companies is to gain control over an entire sector of the economy, such as construction, transportation, or gambling. By using multiple front companies, they can create a network of interrelated businesses that can manipulate prices, evade taxes, and influence public contracts. This can give them a competitive advantage over

legitimate businesses, and allow them to launder large amounts of money through seemingly legitimate transactions.
Another reason why organized crime groups use front companies is to comingle their illicit funds with those of legal businesses. By using the bank accounts of front companies, they can deposit cash from criminal activities along with the revenues from legitimate operations, making it harder to trace the source of the funds. They can also transfer funds between different front companies, or use them to pay for goods and services, creating layers of transactions that obscure the money trail.
Reference:
CAMS Study Guide - 6th Edition, Chapter 2, Section 2.2, page 43
A Guide to the 6th Anti-Money Laundering Directive, Part 2, page 9
Money Laundering and Financial Crimes, Chapter 2, page 29

NEW QUESTION: 241
□□□□□ □□ □□ □□ □□□□□□ □□□ □□□ □□□□□□ □□□□□□ □ □□□ □□ □□ □ □□□ □□□□.
A. □□ □□□□□□.
B. □□ □□ □□□□□□.
C. □□ □□.
D. □□ □□ □□□□□□.
Answer: (SHOW ANSWER)
According to the Anti-Money Laundering Specialist (the 6th edition) study guide, ongoing training is a key element of an effective anti-money laundering compliance program, as it ensures that the staff are aware of their roles and responsibilities, the latest regulatory developments, and the emerging risks and trends in money laundering and terrorist financing1. Ongoing training also helps to foster a culture of compliance within the institution, where the staff are committed to adhering to the policies and procedures, detecting and reporting suspicious activities, and protecting the institution from reputational and legal damages2.
Reference:
1: CAMS Study Guide, 6th Edition, Chapter 2, Section 2.5, page 53
2: CAMS Study Guide, 6th Edition, Chapter 2, Section 2.6, page 54

NEW QUESTION: 242

□□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□□□□?

A. □□□□□ □□ □□

B. □□□ □□□□□□ □□

C. □□ □□□ □□ □□ □□ □□ □□

D. □□□□□□ □□□□□□ □□□□□ □□

Answer: B (LEAVE A REPLY)

Undermining the Legitimate Private Sector: One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers are known to use front companies: businesses that appear legitimate and engage in legitimate business but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the ill-gotten gains. These front companies have a competitive advantage over legitimate firms as they have access to substantial illicit funds, allowing them to subsidize products and services sold at below market rates. This makes it difficult for legitimate businesses to compete against front companies. Clearly, the management principles of these criminal enterprises are not consistent with traditional free market principles, which results in further negative macroeconomic effects

NEW QUESTION: 243

□ □□ □□□ □□ □□ □□ □□ □□□ □□ □□□□ □□□ □□□□ □□□?

A. □□ □□(FI)□ □□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□□□.

B. □□□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□.

C. □ □□ □□□ □□ □□□□ □ □□□ □□ □□ □□□ □□□□□.

D. □□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □.

Answer: A (LEAVE A REPLY)

A compliance officer should cooperate with the law enforcement inquiry as much as possible, but also ensure that the request is valid, lawful, and does not violate any confidentiality or privacy obligations. Therefore, the compliance officer should collaborate with the FI's designated department, such as the legal counsel, the senior management, or the board of directors, to determine the appropriate course of action to comply with the request12. The compliance officer should also ensure that all communication, written and oral, is funneled through a centralized place, and that the FI maintains a record of the request and the response12.

Reference:

1: Requests by Law Enforcement for Financial Institutions to Maintain Accounts, FinCEN, 2014

2: Best Practices for Compliance and Enforcement-Related Information Requests, EPA, 2018

NEW QUESTION: 244

□ □□ □□□ □□ □□□ □□ □ □□ □□ □□□ □□□ □□□ □□□□□□.

□□□□□□ □□□ □□ □□□ □□□ □□□□ □□□?

A. □□□ □□□□ □□ □□□ □□ □□□ □□□□□.

B. □□□ □□ □□ □□ □□ □□□□ □□□ □□□□ □□□ □□□□□.

C. □□□ □□□□ □□ □□□ □□□ □□□□ □□□□□.

D. □□□□□ □□□ □□□ □□□□□□ □□ □□□ □□□□□ □□□□□□.

Answer: B (LEAVE A REPLY)

information

Explanation:

According to the ACAMS Study Guide 6th Edition, Chapter 2, page 37, one of the red flags of money laundering or terrorist financing is the use of nominees, trusts, or third parties to hide the identity, ownership, or control of the funds or assets involved in the transaction. Nominees are individuals or entities that act on behalf of the actual or beneficial owners of a company, trust, or account, and may be used to conceal the source, destination, or purpose of the funds or assets. Nominees may also be used to evade taxes, sanctions, or regulatory requirements.

In this case, the compliance officer is unable to verify the identity of the beneficial owners of the company, and only information on the nominee owners was provided. This raises the suspicion that the company may be involved in money laundering or terrorist financing activities, and that the nominee owners may be acting as fronts or intermediaries for the actual or beneficial owners. The compliance officer should conduct further due diligence on the company, the nominee owners, and the beneficial owners, and report any suspicious or unusual activity to the relevant authorities.

Reference:

ACAMS Study Guide 6th Edition, Chapter 2, page 37

Beneficial Ownership Meaning and Regulation - Investopedia

What is a nominee shareholder? | LawBite

NEW QUESTION: 245

Financial Action Task Force□ □□□ □□ □□□ □□□□□ □□ □ □□ □□□ □□□□□□ □□ □ □□□□□ □□□ □ □□□□□ □□ □□□ □□□ □ □□□ □□□□□□? (2□□ □□□□□□.)

A. □□□ □□ □□□ □□

B. □□□ □□ □□

C. □□□ □□ □□

D. □□ □□ □□ □□

E. □□ □□□ □□□□ □□

Answer: A,D (LEAVE A REPLY)

Here is the exact information from the Financial Action Task Force (FATF) Guidance for a Risk-Based Approach for Trust and Company Service Providers:

"Understanding the management and ownership structure of a trust is crucial in assessing the ML/TF risk it poses. This includes the identity of all settlors, trustees and beneficiaries, and their respective roles and responsibilities, as well as the nature and purpose of the trust."

"TCSPs should obtain and maintain up-to-date information on the purpose and intended nature of the business relationship, the source of funds and wealth, and where relevant, the source of funds or wealth of the settlor and beneficiaries." Based on this information, the correct answers are A and D. Trust and Company Service Providers must understand the responsibility and authority in the structure, as well as the general purpose behind the structure in order to assess the overall risk of the trust and ensure that any transactions with the trust are legitimate.

NEW QUESTION: 246

□□ □□ □□ □□□□ □□□ □□□ □□ □□ □□□ □□ □□ □□ □□ □□ □□, □□ □
□□□ □□□□□ □□□□□□□.
□□ 3□□□ □□□□ □□□? 3□□ □□□ □□□□□

A. □□ □□□□□□□□ □□□ □□□□□ □□
B. □□ □□□ □ □□□ □□ □□ □□□□
C. □□□□□□ □□□□ □□□□, □□ □□ □□□□ □ □□ □□□
D. □□□ □ □□ □□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

these are the essential components of an effective anti-money laundering program for any financial institution, especially an offshore one. According to the CAMS Study Guide, 6th Edition, an anti-money laundering program should include the following elements1:

A risk assessment that identifies and evaluates the money laundering and terrorist financing risks faced by the institution, and the measures taken to mitigate them.

A compliance program that establishes policies, procedures, and controls to prevent, detect, and report money laundering and terrorist financing activities, and to comply with the applicable laws and regulations of the host and chartering countries.

A designated compliance officer who is responsible for overseeing the implementation and maintenance of the compliance program, and for liaising with the relevant authorities and stakeholders.

A training program that provides regular and appropriate education and awareness to senior management and staff on their roles and responsibilities in relation to anti-money laundering and terrorist financing, and on the latest trends and typologies in these areas.

An independent audit function that reviews and tests the adequacy and effectiveness of the compliance program, and reports the findings and recommendations to senior management and the board of directors.

The Basel Committee on Banking Supervision's capital adequacy requirements for the host country (answer A) are not directly related to anti-money laundering, but rather to the prudential regulation and supervision of banks. They are important for ensuring the financial soundness and stability of banks, but they are not sufficient to prevent or combat money laundering and terrorist financing2.

Reference:

1: CAMS Study Guide, 6th Edition, Chapter 5: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), page 139-140. 2: Basel Committee on Banking Supervision, Bank for International Settlements.

NEW QUESTION: 247

□□ □□ □□ □□□ □□□ □□□ □□ □□(CDD) □□ □ □□□ □□□ □□□ □□□ □□ □ □□□□ □□□ □□□□□? (3□□ □□□□□.)

A. □□□ □□□ □□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□ □□□ □□ □□ □□□.

B. □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□□ □ □□□ □□□□ □ □□□□□ □ □□□.

C. □□□ □□□□□ □□ □□□ □□□ □□/□□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□.

D. □□□ □□ □□ □□ □□ □□ □□□ □□□ □ □□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□ □□ □ □□□ □□□□ □□□□ □□□.

E. □□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □ □□ □□□□ □□□.

F. □□□ □□ □□□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□ CDD □□□ □□□□ □□□.

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

According to the Basel Committee on Banking Supervision standards, the following statements best describe sound practices in relation to customer due diligence (CDD) policies and procedures:

Banks should take into consideration the occasional banking transaction or the size/level of assets to build an understanding of the customer's profile and behavior. This is because the nature and frequency of transactions and the size of the account balance may indicate the level of risk associated with the customer and the need for ongoing monitoring1 Banks should develop and implement clear acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of financing terrorism or money laundering. This is because banks should not enter into or maintain relationships with customers who pose unacceptable risks to the bank or the financial system. Banks should also apply a risk-based approach to CDD and apply more stringent measures to higher-risk customers12 Banks should implement enhanced due diligence measures for entering business relationships with high-risk customers, such as approval by senior management. This is because banks should ensure that they have adequate information and controls to manage the risks posed by such customers and to comply with the relevant laws and regulations. Senior management should be involved in the decision-making process and be accountable for the outcomes12

NEW QUESTION: 248

MLAT(□□ □□ □□ □□)□ □□□ □□□□□? (3□□ □□□□□.)

A. MLAT□ □□□□ □□ □□□□□ □□□□ □□□□.

B. □□ □□□□□□ □□ □□□ □□ □□ MLAT□ □□□ □ □□□□.

C. MLAT□ □□ □□□ □□ □□ □□□ □□□□ □□□□.

D. MLAT□□ □ □□□ □□□□□.

E. MLAT□ □□ □ □□□□ □□□ □□□□□.

F. MLAT□ □□□□ □□□ □□□ □□□□ □ □□□□□.

Answer: (SHOW ANSWER)
Mutual Legal Assistance Treaties (MLATs) are characteristics of D. only involving two countries, E. cooperatively combating crime between countries, and F. being useful for gathering evidence and intelligence in a foreign country. MLATs are public and binding under international law (A), can be used for obtaining banking records from treaty partners (B), and provide a legal basis for transmitting evidence ©.

NEW QUESTION: 249
□□□ □ □□□ □□ □□□ □□ □ □□□ □□ □□□ □□□□ □□□□ ABC Holdings Ltd. □ □□ □□ □ $500,000 □□ □□□ □□□□. □□□ □□□ Sunrise Holdings, Ltd□ □□□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□□.
□ □□ □□ □□ □□ □□□ □□□ □ □□□ □□□□ □ □□ □□ □□□ □□□□□?
(2□□ □□□□□.)
A. □□□(□□ □) □□□ □□□□ □□
B. □□□ □□ □□ □□ □□□ □□□□ □□□□.
C. □□□□□ □□□□□ □□□ □□□ □□□□ □□ □□
D. □□□□ □□□ □□□ □□□ □□ □□□□ □□□□ □□□□ □□□ □□□□ □□ □□ □ □□□ □□
Answer: A,D (LEAVE A REPLY)
Trade-based money laundering (TBML) is a method of disguising and moving illicit funds through the international trade system. Criminals often manipulate various aspects of trade transactions, such as pricing, quantity, documentation, and commodity type, to transfer value and obscure the source of funds. Some of the common red flags that may indicate TBML are:
The transaction involves the use of front (or shell) companies: Front or shell companies are entities that have no physical presence, no employees, and no business activity, but are used to facilitate money laundering. They often have vague or generic names, are registered in secrecy jurisdictions, and have no available ownership information. In this case, ABC Holdings Ltd. and Sunrise Holdings Ltd. could be front or shell companies that are used to launder money through trade transactions.
The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities: Criminals may use commodities that are unrelated to their core business or that have low correlation with the market price to launder money. They may also use commodities that are difficult to value, verify, or trace, such as precious metals, gems, art, or antiquities. In this case, the automotive parts company and the silk flower supplier seem to have no logical connection, and the value of the silk flowers may be inflated or deflated to transfer funds.
Reference:
Trade-Based Money Laundering: Risk Indicators - Financial Action Task Force, pp. 9-10, 14-15
Identifying TBML: 8 Trade-Based Money Laundering Red Flags - Alessa, pp. 1-2 FFIEC BSA/AML Appendices - Appendix F - Money Laundering and Terrorist Financing Red Flags, p. 7
AML Red Flags - What are the Top 10 Indicators? - ComplyAdvantage, p. 1

NEW QUESTION: 250

AML □□□ □□□□ □□ □□□□ □□□□ □□□ □□□□□?

A. □□ □□

B. □□□ □□

C. □□ □□

D. □□ □

Answer: (SHOW ANSWER)

Non-compliance with anti-money laundering (AML) laws and regulations can lead to severe consequences for both financial institutions and individuals. One of the indirect consequences is the imposition of punitive fines. These fines can vary based on the type of violation and the institution's willingness to address the issue. Additionally, non-compliance may damage a company's reputation, impacting its standing in the market and potentially leading to financial losses beyond the fines themselves123.

Reference:

Consequences of AML Non-Compliance

Understanding, Consequences & Changes in Anti-Money Laundering

Mastering Compliance: Effective AML Controls for Non-Bank Financial Institutions AML Compliance: The Risks of Poor Practice and What Not to Miss

NEW QUESTION: 251

□□□ □□(EU□ □□□ □□□ □□□ □□)□ □□□ □□□ □□□□ EU □□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□. □□□□ □□ EU □□□ □□□□ □□□□ □□□□ □□□□. □□ □□□ □□ □□□□ □□□ □□□, □□□□ □□ □□ □□ □□□ □□□□□.

□□□□ □□ □□ □□□ □□□□ □□□? (2□□ □□□□□.)

A. □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□□□□□.

B. □□□□ □□□ □□□□ □□ □□ EU □□□ □□□□ □□□□□□□.

C. □□□ □□ □□□ □□□ □□ □□□ □□□ □□□□□□.

D. □□□□ □□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□□□.

Answer: A,D (LEAVE A REPLY)

The real estate sector is a known avenue for money laundering, and this scenario presents multiple red flags.

Option A (Correct): High-risk jurisdictions are associated with corruption and financial crime, making transactions involving their citizens higher risk.

Option D (Correct): Selling assets below market value is a common tactic to disguise illicit funds or transfer value illicitly.

Option B (Incorrect): While cross-border legal representation may raise questions, it is not inherently suspicious.

Option C (Incorrect): Offshore companies are common in tax planning, though they require further scrutiny.

NEW QUESTION: 252

□□□□□□ □□□ □□□ □□, □□□□ □□□ □□□ □ □□□?

A. □□□ □□ □□ □□□ □ □□□ □□□ □□□□□□□

B. □□□ □□□□ □□□□ □□ □□□ □□ □□□ □□□□ □□ □□ □□ □□ □□ □□□ □□□ □□□□□□□

C. □□□ □□□□□□ □□□□□□□

D. □□ □ □□□ □□□□□□□□ □□□□ □ □□□□ □□ □□ □□□□□□ □□□□

Answer: D (LEAVE A REPLY)

A financial institution can verify the nature and purpose of a business and its legitimacy by using an independent information verification process, such as by accessing public and private databases. This method can help the financial institution to check the names of businesses against anti-money laundering (AML) watchlists, parse and analyze ownership information to determine beneficial ownership structure, and run the beneficial owners themselves through identity verification and AML watchlist checks1. This can also help the financial institution to comply with the regulatory requirements for customer due diligence (CDD), which include obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile2. Other methods, such as reviewing a copy of the corporation's latest audited reports and accounts, undertaking a company search or other commercial inquiries, or reviewing the company's website, may not provide sufficient or reliable information to verify the nature and purpose of a business and its legitimacy.

Reference:

Customer due diligence for banks by the Basel Committee on Banking Supervision, October 2001.

How to Verify Legitimate Businesses and Merchants by Trulioo, March 2021.

NEW QUESTION: 253

FATF(Financial Action Task Force)□ □□ □□ □ □□ □□ □□ □□□ □□ □□ □□□ □□ □ □□□ □□□□□?

A. □□ □□

B. FATF □□□□□□

C. □□ □□□

D. □□□ □□ □□ □ FATF□ □□

Answer: A (LEAVE A REPLY)

The FATF measures the effectiveness of a country's efforts to combat money laundering and terrorist financing through a process known as mutual evaluation. This process involves peer reviews, where experts from other member countries assess the technical compliance and the effectiveness of a country's anti-money laundering and counter-terrorist financing (AML/CTF) framework. The FATF has developed a methodology that identifies 11 key areas, or immediate outcomes, that an effective AML/CTF system should achieve, and uses them as the basis for the mutual evaluation. The FATF publishes the mutual evaluation reports, which provide an in-depth

analysis of the strengths and weaknesses of each country's AML/CTF regime, as well as recommendations for improvement.
Reference:
1: An effective system to combat money laundering and terrorist financing, FATF, February 2013.
2: Report on the State of Effectiveness and Compliance with the FATF Standards, FATF, June 2021.
3: Financial Action Task Force (FATF) | Meaning, Functions, Impact, Finance Strategists, September 2023.
4: FATF Recommendations, FATF, October 2020.

NEW QUESTION: 254
□□□□□□□ □, □□ □□ □□□ □□□□ □ □□ □□ □□□□□ □ □□□□□□□ □□□ □ □□□□?
A. □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□□□.
B. □□□ □□□ □□□ □□□□□ □□ □□.
C. □□ □□□□□□ □□ □□□□□ □□ □□.
D. □□ □□□ □□□□□ □□□ □□ □ □.
Answer: B ([LEAVE A REPLY]())
According to the CAMS Certification Package - 6th Edition1, the decision to keep or close an account after filing a suspicious transaction report (STR) should be based on a risk-based approach that considers the nature and severity of the suspicious activity, the customer profile and relationship, the regulatory and legal obligations, and the reputational and operational risks for the institution. The financial impact, the administrative costs, and the number of accounts closed are not the primary factors in determining the appropriate course of action. Therefore, the correct answer is B. Procedures to ascertain the potential risk to the organization.
Reference:
CAMS Certification Package - 6th Edition1, Chapter 5: Risk Management, Section: Account Closure, pp. 211-212.

NEW QUESTION: 255
□□□ □□□ □□□ □ □□□ □□□□□□. □□ □□□ □□ AML □□□ □□□□□ □□ □□ □ □□□□?
A. □□□ □□□ □□□ □□□ □□ □□□□□□□ □□ □□
B. □□□ □□□□□ □ □ □□ □□□ □□□□□ □□□ □□
C. □□□□□□ □□□□□□□ □□□ □□□□□□ □□□□□ □□□□□□ □□□ □□
D. □□□□□ □□□ □3□□□□□ □□ □□ POS □□
Answer: B ([LEAVE A REPLY]())
According to the ACAMS Study Guide for the CAMS Certification Exam (6th edition), page 211, dealers in precious metals and stones (DPMS) are vulnerable to money laundering and terrorist financing risks due to the high value, portability, and fungibility of their products. Therefore, DPMS should apply a risk-based approach to their AML/CFT compliance program and monitor their

customers and transactions for any red flags or suspicious activities. One of the red flags for DPMS is receiving payments from or sending payments to unknown or unverified third parties, especially if they are located in high-risk jurisdictions that have weak AML/CFT controls, are subject to sanctions, or are known to be sources or destinations of illicit funds. Such payments may indicate that the DPMS is being used as a conduit or a front for money laundering, terrorist financing, tax evasion, or other criminal activities. Therefore, if a precious metals dealer opens a new account with a bank and receives or makes payments that reference unknown companies from high-risk jurisdictions, the bank should refer the account to AML investigations for further review and verification of the source and purpose of the funds, the identity and legitimacy of the third parties, and the nature and rationale of the business relationship.

Reference:

ACAMS Study Guide for the CAMS Certification Exam (6th edition), page 2111 FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones2 Risk-Based Approach for Dealers in Precious Metals and Stones (DPMS)3

NEW QUESTION: 256

□□ □□□ □□□ □□□□ □□ SAR/STR□ □□□□ □□□.

A. □□□ □□□ □□ □□□□□.

B. □□ □□□ □□ □□□□ □□□ □□ □□□□.

C. □□□□ □□□□ □□□□ □□ □□□ □□□□□.

D. □□□ □□□ □□□ □□□ □□□□.

Answer: B (LEAVE A REPLY)

According to the ACAMS CAMS Certification Study Guide (6th edition), one of the red flags for money laundering is the structuring of cash transactions to avoid reporting thresholds. Structuring is the practice of breaking down large amounts of cash into smaller deposits or withdrawals that are below the reporting threshold of $10,000 in the United States or equivalent amounts in other jurisdictions. Structuring is done to evade the detection and reporting of cash transactions by financial institutions to the authorities. Therefore, when an accountable institution identifies that a customer is engaging in structuring or other forms of cash transaction manipulation, it should file a SAR/STR to report the suspicious activity1

NEW QUESTION: 257

□□□□□□ □□□ □□(PEP)□ □□□ □□□ □□□□□. □□□ □□□□□ □□□□□ □□ □□ □□ □□□ □□ □□□□□ □□ □□□ □□□ □□□□□□ □□□□□ □□ □□□□□□ □□ □□ □□ □□□□□□□.
□ □□□ □□□□□ □□□□□□□□□□ □□□?
A. □□□
B. □□□ □□
C. □□□ □□□□□□□□□□□
D. □□ □□ □□□□□□□ PEP □□□
Answer: C (LEAVE A REPLY)
According to the ACAMS CAMS Certification Study Guide (6th edition), the bank's anti-money laundering officer is responsible for overseeing the implementation and maintenance of the bank's anti-money laundering program, which includes reporting and escalating suspicious activities involving PEPs. The anti-money laundering officer should be informed of any unusual or potentially illicit transactions involving PEPs, and decide on the appropriate course of action, such as filing additional reports, conducting enhanced due diligence, or terminating the relationship with the PEP. The other options are not correct because they are either not directly involved in the anti-money laundering program, or not the appropriate authority to contact in this situation.

NEW QUESTION: 258
FIU(Financial Intelligence Unit)□ □□ FIU□ □□□ □□□ □ □□□ □□ □ □□ □□□ □□ □□□?
(2□□ □□□□□□.)
A. □□ FIU□ □□□ □□□ □□□□.
B. □□ □□ □ □□ □□
C. □□□ □□□ □□□□□□□□ □□ □□□ □□
D. □□□□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□.
Answer: B,C (LEAVE A REPLY)
According to the Egmont Group of Financial Intelligence Units, which is a global network of FIUs that promotes information exchange and cooperation, FIUs making requests to another FIU should disclose the reason and purpose for the request, and provide feedback on how the information was used12. These actions are intended to enhance mutual trust, transparency, and accountability between FIUs, and to facilitate the effective use of financial intelligence and information for combating money laundering, terrorist financing, and other financial crimes12. FIUs making requests should also respect the confidentiality and data protection requirements of the FIU receiving the request, and avoid imposing unreasonable or unduly restrictive conditions12.
FIUs making requests should not send the same request to all FIUs, as this would be inefficient, unnecessary, and potentially harmful. FIUs should only send requests to FIUs that are relevant and competent to provide the information they need, based on the nature and scope of the case12. Sending the same request to all FIUs could overload the system, create duplication, and compromise the security and confidentiality of the information12. FIUs making requests should

also make best efforts to provide complete and factual information, but this is not an action they should take when submitting a request, but rather when responding to a request from another FIU12.
Reference:
Egmont Group of Financial Intelligence Units Operational Guidance for FIU Activities and the Exchange of Information Principles for Information Exchange Between Financial Intelligence Units

NEW QUESTION: 259
□□ □□ □□□ □□□□ □□ □ □□ □□□ □□□□□□? (2□□ □□□□□.)
A. □□ □□ □□□□ □□ □□ □□
B. □□ □□□ □□ □□ □□□
C. □□ □□□ - □□ 311 - □□ □□
D. □□ □□ □□□□□□ □□□ □ □□□ □□□ □□
Answer: B,D (LEAVE A REPLY)
The U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals. OFAC publishes lists of individuals and entities that are subject to various sanctions programs, such as the Specially Designated Nationals and Blocked Persons List (SDN List), the Sectoral Sanctions Identifications List (SSI List), and the Foreign Sanctions Evaders List (FSE List). These lists are updated frequently and can be accessed through OFAC's website or other sources12.
The Financial Action Task Force (FATF) is an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FATF publishes lists of jurisdictions that have strategic deficiencies in their anti-money laundering and counter-terrorist financing (AML/CTF) regimes, and calls on its members and other countries to apply enhanced due diligence or counter-measures to protect themselves from the risks emanating from these jurisdictions. These lists are updated periodically and can be accessed through FATF's website or other sources34.
Reference:
1: CAMS Certification Package - 6th Edition | ACAMS, Chapter 3: Sanctions, p. 63-64 2: U.S. Department of the Treasury Office of Foreign Assets Control, https://home.treasury.gov/policy-issues/financial-sanctions 3: CAMS Certification Package - 6th Edition | ACAMS, Chapter 4: FATF Recommendations, p. 77-78 4: Financial Action Task Force, http://www.fatf-gafi.org/countries/#high-risk

NEW QUESTION: 260
AML □□ □□ □□□□ □□ □□□□□□□□ □□□ □□ □□□□□□ □□□ □□□ □□ □□□□ □□□ □□□□. □□ □□□ □□□ □□ □□ □□□□□?
A. □□□□ □□
B. □□ □□□□ □□□ □□□□ □□□□□ □□□□
C. □□□□ □□□ □□□ □□□ □□□□.

D. □□ □□□ □□□□□□ □□ □□ □□□□□

Answer: (SHOW ANSWER)

The most appropriate step for an AML compliance officer to take upon receiving notice of government update including the names of the latest terrorists sanctioned by the United Nations Security Council is to update the monitoring software containing sanctioned persons. This is because the AML compliance officer is responsible for ensuring that the financial institution does not engage in any transactions or business relationships with individuals or entities that are subject to sanctions, as this could expose the institution to legal, regulatory, and reputational risks. By updating the monitoring software, the AML compliance officer can ensure that the institution's screening and filtering systems are up to date and can flag any potential matches or hits with the sanctioned persons. This would also enable the AML compliance officer to take appropriate actions, such as blocking or freezing funds, reporting to the relevant authorities, and conducting further due diligence, if necessary.

Reference:

Anti-Money Laundering (AML) | FINRA.org, Overview.

AML Compliance Officer and Their Responsibilities - Tookitaki, Role and Responsibilities of an AML Compliance Officer.

What is an AML Compliance Officer? - Sanction Scanner, Communicate openly with the company's internal management team.

Guidance on Existing AML Program Rule Compliance ... - FinCEN.gov, Financial Institutions Toll-Free Hotline.

NEW QUESTION: 261

EU□ □□□□□□□□□(AMLD)□ □□□□(EU) □□□□ □□ AML □□ □□ □□□ □□□□□? (2□□ □□□□□□.)

A. □□ AML □□ □ □□□ EU AMLD □□ □□□□□ □□□□□□.

B. □□ AML □□□ EU AMLD□□ □□□□□□□ □ □□□ □□ □□□ □□□ □ □□□□.

C. EU AMLD□ □□□□□ □□ AML □□□ □□ □□□□□ □□ □□□□□□□ □□□□□□.

D. EU AMLD□ □□ AML □□□ □□□ □□ □□ □□ □□□□.

E. EU AMLD□ □□ AML □□□ □□□ □□ □□□ □□□ □□□.

Answer: B,C (LEAVE A REPLY)

The EU AMLD provides the legal framework, but member states have discretion in implementation.

Option B (Correct): Countries can impose stricter AML laws than the minimum EU requirements.

Option C (Correct): AMLDs set the foundation, and member states implement local laws.

Option A (Incorrect): EU law takes precedence, and national laws must align with it.

Option D (Incorrect): AMLDs and local AML regulations are interlinked.

Option E (Incorrect): National AML rules do not have to be identical across all EU members.

NEW QUESTION: 262

□□□□ □□□□ □□ □□ □□□□□□ □□□ □□□□□ □□□?

A. □□□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□□.
B. □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□
C. □□ □□□□ □□
D. □□□□□□ □□ □□
Answer: C (LEAVE A REPLY)
An effective anti-money laundering training program should include real-life money laundering examples to illustrate the concepts and strategies for detecting and preventing money-laundering activity. Real-life examples can help employees to understand the risks, methods, indicators, and impacts of money laundering, as well as the roles and responsibilities of different staff members in combating it. Real-life examples can also enhance the engagement, retention, and application of the knowledge gained from the training program.
Reference:
The document titled "Anti-Money Laundering Awareness Training" published by ACAMS. You can access it by clicking here. This document states that "ACAMS AML General Awareness Training equips employees with knowledge of basic anti-money laundering (AML) principles" and that it is "based on real-life industry scenarios with interactive content to help learning stick".
The document titled "Anti-Money Laundering (AML) Training" published by LIMRA. You can access it by clicking here. This document states that "LIMRA's AML training program provides training for insurance and securities producers and home office employees" and that it "uses real-life scenarios to help learners understand how to apply AML principles to their everyday work".

NEW QUESTION: 263
Wolfsberg Group□ □□ □□ □□ □□□ □□ □□□□□□ □□ □□ □□□ □□□□□□ □□□ □□ □□□□□□?
A. □□□□ □□
B. □□□ □□
C. □□ □□
D. □□□□
Answer: C (LEAVE A REPLY)
Alternative remittance, also known as underground banking or informal value transfer systems, is a method of transferring money or value without using formal financial institutions or channels. It is often used by migrant workers, refugees, or people who lack access to formal banking services. However, it can also be exploited by criminals and terrorists to move funds across borders without detection or regulation. The Wolfsberg Group, a group of leading international banks that promotes best practices in anti-money laundering and counter-terrorist financing, cited alternative remittance as one of the sectors and activities that are widely used for the financing of terrorism in its Statement on the Suppression of the Financing of Terrorism. The Wolfsberg Group recommended that financial institutions apply enhanced and appropriate due diligence to customers engaged in alternative remittance and report any suspicious transactions to the relevant authorities.
Reference:

Wolfsberg Group (2002). Wolfsberg Statement on Anti-Terrorism Financing1 Pieth, M. (ed.) (2002). Financing Terrorism. Springer, Dordrecht2 ACAMS (2020). CAMS Certification Package (6th Edition)3

NEW QUESTION: 264

□□ □□□□□ □□□ □□ □□ □□ □□□ □□ □□ □□□□□□ □□□?

A. □□□□□ □□□ □□□□□ □□□ □□□ □ □□□ □□□ □□□□□ □□□.

B. □□ □□ □ □□□□ □□□□□ □□ □□ □□□□□□ □□□□□□.

C. □ □□□ □□ 20□□ □□□ □□□□□□ □□□ □□ 500□□ □□□□□□.

D. □□□□□ □□□ $1,000 USD □□□ □□□□□ □□□ □□ □□ □□□ □□□□□□□.

Answer: (SHOW ANSWER)

This is a common red flag of money laundering that involves layering, which is the process of moving funds through multiple accounts or entities to conceal their origin and ownership. Layering often involves cross-border transfers, especially to high-risk jurisdictions, and rapid movement of funds to avoid detection or tracing. A compliance officer should prioritize this red flag for investigation, as it may indicate a complex money laundering scheme or the financing of terrorism or proliferation.

Reference:

AML Red Flags - What are the Top 10 Indicators? - ComplyAdvantage, section "Red flags related to transaction patterns" AML 101: The 10 Most Common Red Flags - KYC-Chain, section "Red flag indicators related to geographical risks" Anti-money laundering red flags, page 2, bullet point 5

NEW QUESTION: 265

□□ □□(FI)□ □□ □□ □□□□□ □□ □□ □□□□□□ □□□□□□ □□□□□□□. FI□ □□□ □□ □□ □□ □□ □□□□□□ □□□ □□ □□□ □□□□□ □□□?

A. □□□ □□

B. □□ □□

C. □□□□□ □□

D. □□□ □□

Answer: D (LEAVE A REPLY)

A risk-based compliance program is one that identifies and prioritizes the highest compliance risks to the FI and implements controls, policies and procedures to mitigate them. A data-based option is the most suitable for a risk-based compliance program, as it allows the FI to collect, analyze and monitor relevant data on its customers, transactions, products, services, geographies and other risk factors. A data-based option also enables the FI to measure the effectiveness of its compliance program and adjust it as needed to respond to changing risks and regulatory expectations12.

Reference:

1: Risk-Based Approach to Compliance Management2

2: A Risk-Based Approach to Regulatory Compliance1

NEW QUESTION: 266
□□ □□ □□□ USA PATRIOT Act□ □□ □□ □ □□□ □□□□ □□ □□□ □□□ □ □□ □ □□□□?
A. □□□□
B. □□□□
C. □□□□
D. □□□□
E. S. USA PATRIOT Act□ □□ □□□ □ □□ - Exam-Answer3
Answer: B (LEAVE A REPLY)
Correspondent banking is the product type that is subject to US extra-jurisdictional reach over non-US banks and non-US persons under the USA PATRIOT Act. This is because correspondent banking involves the provision of banking services by one bank (the correspondent) to another bank (the respondent) or to the respondent's customers. Correspondent banking enables cross-border transactions and access to foreign financial systems, but also poses significant money laundering and terrorist financing risks due to the lack of transparency and accountability of the parties involved. The USA PATRIOT Act requires US financial institutions to apply enhanced due diligence measures to correspondent accounts for certain foreign banks, such as those operating under offshore banking licenses, those owned or controlled by foreign governments, or those of primary money laundering concern. These measures include obtaining information about the ownership, management, and anti-money laundering controls of the foreign bank, as well as the identity and activity of the customers using the correspondent account. The USA PATRIOT Act also authorizes the US Treasury to prohibit or impose conditions on the opening or maintaining of correspondent accounts for foreign banks that are involved in money laundering or terrorist financing activities.
Reference:
CAMS Study Guide, 6th Edition, Chapter 5, Section 5.2.1, p. 1611
Financial Crimes Enforcement Network; Anti-Money Laundering Programs; Special Due Diligence Programs for Certain Foreign Accounts, 31 CFR Part 103, RIN 1506-AA292

NEW QUESTION: 267
□□□□□□ □□□□ □□□□ □□□□ □□□□ □□. □□□□ □□□ □□□□□ □□□ □ □□ □□□□ □□ □□ □□ □□□□□?
A. □□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□ □□□□□.
B. □ □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□□□□.
C. □□□□□□□, □□□ □□□□ □□
D. □□□ □□□ □□□ □□
Answer: C (LEAVE A REPLY)
An automated transaction monitoring system is a tool that analyzes transactions and customer behavior for signs of money laundering or other financial crimes, and generates alerts when suspicious or unusual activity is detected. The system relies on a set of rules and parameters that

define what constitutes normal and abnormal transactions, based on the risk profile and business nature of the financial institution or business. These rules and parameters need to be periodically reviewed and updated to ensure that they are effective and compliant with the latest regulations and best practices.

One of the factors that would most likely result in a change in the monitoring system parameters is when the national Financial intelligence Unit (FIU) issues new risk indicators. The FIU is a central authority that collects, analyzes, and disseminates financial intelligence related to money laundering, terrorist financing, and other financial crimes. The FIU also provides guidance and feedback to financial institutions and businesses on how to comply with their anti-money laundering (AML) obligations and improve their transaction monitoring systems. The FIU may issue new risk indicators based on its analysis of emerging trends, typologies, and threats in the financial sector, or based on international standards and recommendations. These risk indicators are intended to help financial institutions and businesses identify and report suspicious transactions more effectively and efficiently.

Therefore, when the FIU issues new risk indicators, the financial institution or business should review its existing monitoring system parameters and adjust them accordingly to reflect the new risks and scenarios. For example, the FIU may issue new risk indicators related to the use of cryptocurrencies, virtual assets, or online platforms for money laundering or terrorist financing. In that case, the financial institution or business should update its monitoring system parameters to include new rules, thresholds, or patterns that capture these activities and generate alerts for further investigation.

Reference:

1: The Complete Guide to Transaction Monitoring: Everything to Know

2: AML Scenarios: Transaction Monitoring Challenges

3: Setting AML Transaction Monitoring Thresholds

4: Automated Transaction Monitoring - Considerations for System Implementation

5: ACAMS (2020). CAMS Certification Package (6th Edition)

NEW QUESTION: 268

2012□ □□□□□□□(FATF)□ 40□□ □□□□ □/□□ 11□□ □□□ □□□ □□ □□ □□ □ □□ □□ □□□□□□?

A. 40□□ □□□□□□ □□□ □ □□□□□□ □□ □□ □□ □□□ □□□□ □□□□.

B. □ □□□□□□□ FATF□ □□□□ 40□ □□ □□□ □□ □□ □□□ □□ □□□ □□□ □ □□ □ □□□□.

C. 40□□ □□□□□□ □□□ □□□ □□□ □□□□□□ □□□□□□□ □□□□□□.

D. 11□□ □□□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □ □□□□.

Answer: A (LEAVE A REPLY)

The FATF 40 Recommendations provide a global AML/CFT framework, and the Immediate Outcomes assess effectiveness.

Option A (Correct): The risk-based approach (RBA) is the foundation of modern AML compliance and is mandated by FATF Recommendation 1.
Option B (Incorrect): Interpretive notes are public documents available to all jurisdictions, not private.
Option C (Incorrect): The 40 Recommendations are regularly updated, incorporating new technology (e.g., virtual assets in 2019).
Option D (Incorrect): The 11 Immediate Outcomes assess the effectiveness of AML systems globally, not just for high-risk countries.

NEW QUESTION: 269

□□□ □□ □□ □□ □□□□□ □□□□□ □□ □□ □□ □□□ □□□□□ □□□ □ □□□□□ AML □□□□□ □□□□□□ □□□ □□□ □□□.

A. □□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□□□.
B. □□□ □□□ □ □□ □□□ □□ □□□□□□.
C. □□ □□□ □□□□□ □□□.
D. □□ □□ □□□ □□□□□ □□ □□□ □□□□□□□.

Answer: D (LEAVE A REPLY)

When assessing and managing money laundering risks while operating in foreign jurisdictions different from that of the head office, an effective AML monitoring program should conform to the foreign jurisdiction policies to align with the head office policies. This ensures that the organization's AML/CFT risk management remains consistent across all jurisdictions, while allowing local compliance staff to assess and manage the risks specific to their jurisdiction. Additionally, the program should be tailored to the higher of standards between the jurisdictions, and should be consistent with the head office audits. Providing all foreign jurisdiction reports to the head office for approval is not necessary, as long as the program is consistent with the head office policies.

NEW QUESTION: 270

□□ □ □□ □□□□□ □ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□ □ □□□□? (2□ □ □□□□□□.)

A. □□□□□□ □□□□□□□ □□□ □□□ □□□ □□
B. □ □□ □□□ □□ □□ □□ □□□□□ □□□□□ □□
C. □□□ □□□□□□ □□□□□□ □□□ □□
D. □□□□□□ □□□□□□ □□□ □□ □□□□□□ □□ □□

Answer: (SHOW ANSWER)

Q Law enforcement may be given access to a financial institution customer's financial records if they serve a legal summons or subpoena, or if they have circumstantial evidence to suspect money laundering. These are two of the exceptions to the general rule that financial institutions must protect the privacy of their customers' financial information under the Right to Financial Privacy Act (RFPA) of 19781. The RFPA also allows access to customer records in other

situations, such as with the customer's consent, in response to judicial orders, or for certain intelligence or counterintelligence purposes1.
Option A is incorrect because a suspicious transaction report (STR) does not automatically grant law enforcement access to the customer's financial records. The STR is a confidential document that is filed by the financial institution to the Financial Intelligence Unit (FIU) of the country, and the FIU may decide to share the information with law enforcement if it deems appropriate2. However, law enforcement still needs to follow the RFPA procedures to obtain the customer's records from the financial institution.
Option C is incorrect because the investigation of a customer being made public in the media does not give law enforcement the right to access the customer's financial records. The media exposure may raise the public interest or the urgency of the investigation, but it does not override the RFPA requirements. Law enforcement still needs to obtain a legal summons, subpoena, or other valid authorization to access the customer's records from the financial institution.
Reference:
1: Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 2: ACAMS Study Guide for the CAMS Certification Examination, 6th Edition, Chapter 2: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), p. 47

NEW QUESTION: 271
□□□□□□ □□□ □□□□□□□ □ □□□ □□ □□□□ □□□□ □□□ □□□ □□□□?
A. □□□ □□□ □□□ □□□□□□ □□
B. □□□ □□□□ □□ □□
C. FIU□ □ □□□ □□ □□□ □□□□ □□
D. □□□ □□□ □□ □□ □□ □□ □□ □□
Answer: D (LEAVE A REPLY)
"Transaction Monitoring Systems and Ongoing Monitoring: Since the transactional monitoring system is key to mitigating ML risk within the bank, the Committee recognizes that AML risks require more than just appropriate policies and procedures; banks must have adequate and appropriate monitoring systems. For most banks, this will involve an IT monitoring system. If the bank does not believe it needs an IT monitoring system, it should document the rationale for why it does not need one.

NEW QUESTION: 272

□□ □ □□□ □□ □□(EDD)□ □□□ □□□□□□ □□□□□? (□ □□□ □□□□□.)

A. 25□ □ □□□ □□□ □□□ □□□ □ □□□□□□ □□ □□□ □□□ □□□□□ □□□ □□ □□□□.

B. □□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□□□ □□□ □□□□□□ □□.

C. □□□□□ □□ □□□ □□□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□ □□ □ □□□□□□ □□□□□.

D. □ □□□ □□□□□□ □□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□□ □□ □□.

E. □□ □□□□□ □□ □□□ □□□□□□ □□□ □ □□.

Answer: (SHOW ANSWER)

Enhanced Due Diligence (EDD) applies to high-risk customers and transactions, including politically exposed persons (PEPs), high-risk jurisdictions, and correspondent banking relationships.

Option C (Correct): Correspondent banking relationships with high-risk jurisdictions require EDD to prevent cross-border financial crime.

Option D (Correct): Ambassadors are considered PEPs, which require EDD due to corruption risks.

Option E (Correct): A current prime minister is a high-profile PEP, requiring EDD and ongoing transaction monitoring.

Why Other Options Are Incorrect:

Option A (Incorrect): The individual no longer holds a PEP position and is in a low-risk country, so EDD is not required.

Option B (Incorrect): A local footballer does not present a high financial crime risk warranting EDD.

EDD Best Practices for High-Risk Customers:

Verify the source of wealth and funds for PEPs.

Conduct ongoing transaction monitoring on high-risk accounts.

Apply stricter controls on correspondent banking with high-risk jurisdictions.

Reference:

FATF Recommendation 10 & 12 (EDD & PEPs)

Basel Committee's Correspondent Banking Guidelines

Wolfsberg Group Guidance on High-Risk Customers & EDD

NEW QUESTION: 273

□□□ □□□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□□□ □□ □□□ □□□□□. □ □□ □□□ □□□□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□□□.

□ □□□ □□□ □□ □□□ □□□ □□□□□ □□□□□□ □□□□□□ □□□ □□□□□ □□□ □.

□□ □□□ □□□□□ □□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□ □□□□□ □□□ □□□□□□□.

□□□□□ □□□ □□ □□□ □□□ □□□?

A. □□□ □□□□□ □□□ □□□□□□.

B. □□□ □□□ □□□□ □□□ □□□□□.
C. □□ □□□ □ □□ □□□ □□□□□□□.
D. □□□ □□ □□□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
it describes the action that the anti-money laundering specialist should take next, which is to consult with senior management and the legal advisor. This is because the specialist needs to seek guidance and approval from the higher authorities and the legal experts on how to handle the situation without compromising the ongoing criminal investigation or violating the anti-money laundering laws and regulations. The specialist also needs to ensure that the institution's internal policies and procedures are followed and that the appropriate measures are taken to mitigate the risks and protect the reputation of the institution.
The other options are not necessarily actions that the anti-money laundering specialist should take next, although they may be considered or implemented later depending on the outcome of the consultation and the investigation. Option A describes a possible consequence for the employee, which is to recommend the immediate termination of the employee, but this may not be the best course of action at this stage, as it may alert the employee or the dealer of the investigation, or it may be premature or disproportionate without sufficient evidence or due process. Option B describes a possible measure for the dealer, which is to advise that the dealer's accounts should be closed, but this may not be feasible or advisable at this stage, as it may also tip off the dealer or the employee of the investigation, or it may interfere with the collection of evidence or the prosecution of the case. Option D describes a possible reporting obligation for the institution, which is to inform the institution's regulatory agency of the situation, but this may not be required or appropriate at this stage, as it may conflict with the instructions of the competent authority or the confidentiality of the investigation, or it may expose the institution to legal or regulatory liabilities or sanctions.
Reference:
ACAMS CAMS Certification Video Training Course - 6th Edition1
Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)2 ACAMS CAMS Study Guide - 6th Edition, Chapter 6, pages 132-133
: https://www.acams.org/wp-content/uploads/2019/09/ACAMS-CAMS-Study-Guide-6th-Edition-Chapter-6.pdf

NEW QUESTION: 274
□□ □□ □□□ □□□□ □□ □□□□ □□□ □□ □□ □□ □ □□ □□ □□□ □□□□□ □□□ □ □□□□? (3□□ □□□□□.)
A. □□□□□ □□□ □□□ □□ □□ □□
B. □□□□ □□□ □□□, □□, □□□□ □□ □□□ □□ □□□ □□□□ □□□ □□□□ □.
C. □□ □□□□ □3□ □□ □□□□ □□□□□ □□□□□.
D. □□ □□□ □□□□□ □□□□ □□□ □□□ □□□ □□.
E. □□ □ □□ □□ □□□□ □□□□ □□□ □□ □□□ □□□□□.

F. S. FinCEN□ □□ □ □□ □□ □□ AML □□□ □□ □□

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

The art and antiquities market is highly vulnerable to money laundering and terrorist financing due to anonymity in transactions, lack of regulatory oversight, and difficulty in tracing ownership.

Option A (Correct): Art storage in tax-free zones can be used to obscure ownership and avoid AML scrutiny.

Option C (Correct): Using third-party art advisors can facilitate anonymous transactions and shield beneficial ownership.

Option D (Correct): High-value art sold on social media without proper provenance raises ML/TF risks due to lack of financial oversight.

Why Other Options Are Incorrect:

Option B (Incorrect): Paying fair market value does not indicate illicit activity-underpricing or rapid resale are bigger red flags.

Option E (Incorrect): Authenticity verification is common in legitimate art transactions and is not a direct ML/TF red flag.

Red Flags for Art & Antiquities Money Laundering:

Frequent high-value art transactions with no clear business purpose.

Use of intermediaries to conceal beneficial ownership.

Rapid resale of newly purchased art at below-market prices.

Best Practices for AML in the Art Market:

Conduct enhanced due diligence (EDD) on high-value art transactions.

Monitor transactions involving politically exposed persons (PEPs).

Report suspicious transactions linked to high-risk art traders.

Reference:

FATF Report on Money Laundering in the Art & Antiquities Market

6th EU AML Directive (6AMLD) on High-Value Asset Transactions

NEW QUESTION: 275

□□□□ □□□ □□ □□ □□ □□□ □□□□ □□□□ □□ □□□□ □□□□□. □□ 1□ □□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□□□□. □□□□□ □ □□ □□□ □□□□ □□□□ □□ □□ □□□□.

□□□ □□ □□□□ □□ □□□ □□□□□ □□□?

A. □□ □□ □□ □□ □□□ □□□ □□□□□.

B. □□ □□ □□ □□□ □□ □□□ □□

C. □□ □□ □□□ □□□□ □□□□ □□ □□

D. □□□ □□□ □□ □□ □□ □□□ □□□□ □□□□□ □□□□□.

Answer: C (LEAVE A REPLY)

Reviewing parameter settings based on the latest risk assessment should be included in the evaluation of system settings for anti-money laundering alert surveillance. This is because parameter settings determine the thresholds and criteria for generating alerts based on the risk profile of the customers, products, services, channels, and jurisdictions involved in the

transactions. A risk assessment is a periodic and comprehensive analysis of the potential money laundering and terrorist financing risks faced by an organization, and it should inform the design and implementation of an effective anti-money laundering program, including the alert surveillance system. By aligning the parameter settings with the risk assessment, an organization can ensure that the system is capturing the most relevant and high-risk transactions, and reducing the number of false positives or irrelevant alerts.
Reference:
CAMS Study Guide 6th Edition, page 37-38.
Implementing AML Transaction Monitoring Systems: Critical Considerations, page 2-3.
3 techniques to improve AML transaction monitoring strategies, page 2.

NEW QUESTION: 276
□□ □ □□□ □□□ □□ □□□ □□□□□ □□□□□ □□□□ □□ □□□□ □ □□□ □□ □□□?
A. □□□□□ □□□□□ □□□ □□□ □□□ □ □□□ □□
B. □ □□ □□□ □□ □□ □□□ □□□ □□
C. □□ □□ □□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□ □□□ □ □□□ □□
D. □ □□ □□ □□□ □□□□ □□□ □□□ □□ □□□ □□□□ □□□ □□
Answer: C (LEAVE A REPLY)
According to the ACAMS CAMS Certification Study Guide (6th edition), one of the challenges of information sharing within a financial group is the compliance with privacy and data protection rules that may vary across jurisdictions. Therefore, before sharing information about a customer with an affiliate, a bank should consider whether such sharing is permitted by the applicable laws and regulations, and whether the customer has consented to it. The other options are not relevant factors for information sharing in the case of an investigation.

NEW QUESTION: 277
□□ □□□ □□(MSB)□ □□ □□□ □□□ □ □□ □ □□ □□□ □□ □□ □□ □□□ □□ □□□? (2□□ □□□□□.)
A. □□ □□□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□ □□.
B. □□□□□□ □□□□ □ □□□ □□ □□□□ □□□□□□ □□ □□□ □□□□ □□.
C. □□□□ □□□ □□ □□□ □□ □□ □□.
D. □□ □□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.
E. □□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
MSBs are high-risk for financial crime, requiring strict AML controls.
Option D (Correct): Hesitancy to provide beneficiary information is a strong indicator of illicit financial activity.
Option E (Correct): Using multiple accounts under different names is a known money laundering technique.

Option A (Incorrect): Currency exchange is common in MSBs, though additional factors must be assessed.
Option B (Incorrect): Large cash deposits are normal for cash-based businesses, but need further scrutiny.
Option C (Incorrect): Frequent small remittances are normal, unless linked to structuring or smurfing.

NEW QUESTION: 278
□□□ □□ □□□ □□□□ AML □□□ □□□□ □□ □□ □□□ □□□ □□□?
A. □□ □□□□□□ □□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□□□.
B. □□□ □□□ □□□□□ □□ □□□□ □□ □□ □□ □□□ □□□□□.
C. □□ □□□□ □□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□□□.
D. □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
According to the FATF Recommendation 40, which sets the standards for international cooperation in relation to money laundering, associated predicate offences and terrorist financing, countries should ensure that exchanged information is used only for the purpose for which it was sought or provided, and that any dissemination or use of the information beyond the original scope is subject to prior authorization by the requested competent authority. Moreover, countries should have safeguards in place to ensure that the information exchanged is protected in a manner that is consistent with the way they protect their own information of a similar nature. One of the possible safeguards is to require the use of non-disclosure agreements or other legal instruments to prevent unauthorized access or disclosure of the exchanged information.

NEW QUESTION: 279
□□ □□□ □□□□ □□ □□□□□ □□□ □□ □□ □□ □□□ □□□□.
□□□□ □□ □□□ □□□ □□?
A. □□□□□□ □□□ □ □□□ □□□□□.
B. □□□ □□ □□ □□□□ □□□ □□ □ □□
C. □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□□□
D. □□ □□ □□□□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
program
Explanation:
The board of directors is ultimately responsible for ensuring that the financial institution has an effective anti-money laundering program that complies with the applicable laws and regulations. If the institution receives a regulatory enforcement action, the board should take prompt and corrective actions to address the deficiencies and mitigate the risks of further violations or penalties. One of the most important actions is to instruct the compliance officer to develop a plan to remediate the institution's anti-money laundering program, which should include a root cause analysis, a gap assessment, a timeline, and a budget. The board should also monitor the

implementation and progress of the remediation plan, and communicate with the regulators on a regular basis.
The other options are not appropriate actions for the board of directors to take in response to a regulatory enforcement action. Terminating the compliance officer and staff may not solve the underlying issues of the anti-money laundering program, and may create more disruption and instability. Purchasing and installing a new suspicious activity monitoring system may not be necessary or sufficient to address the deficiencies, and may entail additional costs and challenges. Hiring an attorney to protest the enforcement action may not be in the best interest of the institution, and may antagonize the regulators and escalate the situation.
Reference:
CAMS Certification Package - 6th Edition | ACAMS, Chapter 5: Risk Management, Section 5.2: Regulatory Examinations and Enforcement Actions, pp. 171-174.
CAMS Certifications: How to Get CAMS Certified | ACAMS, CAMS Examination Preparation Guide, Section 3: Regulatory Compliance, pp. 23-24.

NEW QUESTION: 280
□□ □□ □□ □ □□□□ □□□ □□ □□ □□ □□□□□?
A. □□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
B. □□□□ □□ □□□□ □□□ □□□□□ □□□□□.
C. □□ □□ □□□□ □□ □□ □□□□ □□ □ □□□ □□□□□□.
D. □□ □□ □□□ □□ □□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The customer activity that poses the highest risk of money laundering is making multiple cash deposits slightly below a required reporting limit. This could indicate a practice known as structuring or smurfing, which is a method of breaking down large amounts of cash into smaller transactions to avoid detection or reporting by financial institutions12. Structuring is a common technique used by money launderers to conceal the source, ownership, or destination of illicit funds3.
The other options are not necessarily indicative of money laundering, although they may require further due diligence or monitoring depending on the customer profile and the nature of the transaction. For example:
Transferring funds to pay for flight training lessons could be a legitimate educational expense, or it could be related to terrorist financing or other criminal activities. The financial institution should verify the identity and background of the customer and the recipient, and check for any red flags or suspicious indicators4.
Paying a supplier of precious metals at regular quarterly intervals could be a normal business practice, or it could be a way of moving or storing value in an alternative asset class. The financial institution should assess the customer's source of funds, business rationale, and market conditions, and monitor for any changes or inconsistencies.
Conducting business in a country that represents a high risk of money laundering could be a legitimate commercial opportunity, or it could be a sign of involvement in illicit activities or tax

evasion. The financial institution should apply enhanced due diligence measures, such as verifying the identity and reputation of the customer and the counterparties, obtaining information on the purpose and nature of the business relationship, and screening for any sanctions or adverse media.
Reference:
ACAMS CAMS Certification Video Training Course - Exam-Labs3
Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)4 ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 2, page 29: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-2.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 6, page 121: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-6.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 7, page 139: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-7.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 4, page 77: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-4.pdf

NEW QUESTION: 281
□□□ □□□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□?
A. □□ □□ □□□(BSA)□ □□□ □□ □□□ □□ □□□ □□ USD □□□ □□□□ □ □□ □□ □□ □□□ □□□□□ □□ □□□□□.
B. 2020□ □□□□□□□(AML□)□ □□ □□ □□□ □□ □□ □□□ □□ USD □□□ □□ □□□.
C. □□ □□□ □ 319□(b)□□ □□ □□□ □□ □□□□ □□□ □□ □ □□ □□ □□□□ □ □□ □□□□ □□ □□□□□.
D. □□□□□□□(OFAC)□ □□ □ □□ □□□ □□ □□□ □□ □□ □ □□□ □□ □□ □ □□ □□□ □ □□□□.
E. S. AML □□ □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□□.
Answer: C,D (LEAVE A REPLY)
Option C (Correct): Section 319(b) of the USA PATRIOT Act allows the seizure of funds from foreign correspondent bank accounts in the U.S.
Option D (Correct): OFAC sanctions can affect non-U.S. entities if they engage in prohibited transactions using U.S. dollars.
Option A (Incorrect): The Travel Rule applies only to financial institutions under U.S. jurisdiction.
Option B (Incorrect): The AML Act of 2020 strengthens U.S. financial crime enforcement, but does not govern all USD transactions worldwide.

NEW QUESTION: 282
□□□ □□ □□ □□□□□ □ □□ □□□ □□□□□?
A. □□□□□ □□ □□□ □□□ □□□□ □□
B. □□ □□□ □□□□ □□□ □□□ □□ □□
C. □□□□□ □□□□ □ □□ □□

D. □□□□ □□ □□ □□□□ □□ □□□□ □□□□□□ □□□ □□

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

A sound Customer Due Diligence Program (CDD) is a key component of an effective anti-money laundering and counter-terrorism financing (AML/CFT) framework. According to the Financial Action Task Force (FATF), the global standard-setter for AML/CFT, CDD involves the following elements1:

Identifying the customer and verifying their identity using reliable, independent sources of information or documents.

Identifying the beneficial owner and taking reasonable measures to verify their identity, so that the financial institution understands who ultimately owns or controls the customer or the funds.

Understanding and obtaining information on the purpose and intended nature of the business relationship.

Conducting ongoing due diligence on the business relationship and scrutinizing transactions to ensure that they are consistent with the financial institution's knowledge of the customer, their business and risk profile, and the source of funds.

Therefore, the three elements of a sound CDD program that are listed in the question are:

Determination of what type of customer the financial institution will accept: This involves defining the customer acceptance policy and risk appetite of the financial institution, and applying appropriate risk-based measures to accept or reject customers based on their risk profile and the financial institution's ability to manage and mitigate those risks2.

Training as to how and to what extent to identify prospective customers: This involves providing adequate and regular training to the staff who are responsible for conducting CDD, and ensuring that they are aware of the legal and regulatory requirements, the internal policies and procedures, the risk indicators, the verification methods, and the reporting obligations3.

Obtaining date of birth and address of a prospective customer: This is part of the basic information that is required to identify and verify the customer's identity, and to establish their risk profile and the source of funds. The date of birth and address can also be used to check against various databases and watchlists to detect any potential matches with sanctioned or high-risk individuals or entities4.

The element that is not part of a sound CDD program is:

Determination of who in the institution should be assigned to the prospective customer as a liaison: This is not a mandatory or essential element of CDD, although it may be a good practice to assign a dedicated relationship manager or contact person to each customer, especially for high-risk or complex customers, to ensure effective communication, monitoring, and service delivery.

Reference:

FATF Guidance on Customer Due Diligence and Financial Inclusion 1

ACAMS Study Guide for the CAMS Certification Examination (6th Edition), Chapter 2: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) 2 ACAMS Study Guide for the CAMS Certification Examination (6th Edition), Chapter 4: Developing an AML/CFT Program 3 ACAMS Study Guide for the CAMS Certification

Examination (6th Edition), Chapter 5: Conducting and Supporting the Investigation Process 4 Wolfsberg Group Guidance on Customer Due Diligence (CDD)

NEW QUESTION: 283
□□□ □□ □□□□□ □□ □□ □□ □□ □□ □□□□□ □□□ □□□ □□□ □□□ □□ □□
□□ □□□ □□□ □□□□. □□□ A □□□□ □ □□□□□ □□□□ □□□ A □□□ □□□
□□.
□□□ □ □ □□□ □□□□ □□ □ □□ □□□ □□□ □□□□ □ □ □□□□ B □□□ □□
□ □□□□□ □□□ □□□ □□□ □□□□□□.
□ □□ □□□ □ □□□ □□ □□□ $8,000□□□.
□ □□□ □□ □□ □□□□ □□ □□□□□□ □□□ □□□ □□□?
A. □□□□□ □□
B. □□□□ □ □ □□ □□□.
C. □□□ B□□□ □□□□ □□□ □□□□
D. □ □□□ □□ □□ □□□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
This involves breaking down large amounts of cash into smaller transactions that are below the reporting threshold of $10,000 in the United States, in order to avoid detection and reporting by the financial institution. Structuring is a red flag for money laundering and should be reported to the authorities as a suspicious activity. The other options are not necessarily indicative of money laundering, as they could have legitimate explanations. For example, the customers may have a family or business connection to the same recipient in Country B, or they may have a regular need to send money three times a week.
Reference:
ACAMS CAMS Certification Video Training Course, Chapter 2: Money Laundering Risks and Methods, Section 2.2: Common Money Laundering Techniques Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition), Question 91 CAMS Certification Package - 6th Edition, Study Guide, Chapter 2: Money Laundering Risks and Methods, Page 38

NEW QUESTION: 284
□□ □ □ □□ Financial Action Task Force □□□□□□ □□□□ □□ □□□□□?
A. □□□□□ □□ 40□□ □□□□
B. □□□ □□ □ □□□ □□ □□□
C. □□□□ □□□ □□ □□□
D. □□ □□ □□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
The first Financial Action Task Force (FATF) initiative was the 40 Recommendations on Money Laundering, which were issued in April 1990, less than a year after the FATF was established by the G7 summit in Paris in 1989. The 40 Recommendations aimed to provide a comprehensive plan of action to fight money laundering by setting out the principles and measures for effective legal, regulatory, and operational frameworks at the national and international levels. The 40

Recommendations have been revised and updated several times since then, most recently in 2022, to reflect the evolving trends and techniques of money laundering and to include the issues of terrorist financing and the financing of proliferation of weapons of mass destruction.
The other options are not the first FATF initiative, but they are related to the FATF's work and mandate. The Report on Non-Cooperative Countries and Territories (NCCTs) was launched in 2000 to identify and monitor the jurisdictions that did not comply with the FATF standards and posed a risk to the international financial system. The Report on Money Laundering Typologies was first published in 1996 and has been updated annually to provide an analysis of the methods, techniques, and trends of money laundering and to assist the FATF members and observers in developing effective countermeasures. The Special Recommendations on Terrorist Financing were issued in October 2001, following the September 11 attacks, to complement the 40 Recommendations and to address the specific challenges of combating the financing of terrorism and terrorist acts.
Reference:
History of the FATF, 1
Financial Action Task Force - Wikipedia, 2
Financial Action Task Force (FATF): What it is, How it Works - Investopedia, 3 The FINANCIAL ACTION TASK FORCE (FATF) - INSIGHTSIAS, 4

NEW QUESTION: 285
□□□ □□ □□□ □□□□ STR□ □□□ □ □□□ □□ □□□ □□□ □□ □□□ □□□□ □?
A. □□□ □□□ □□ □□□ □□□ □□□□ □□□.
B. □□□ □□□ □□ □□□□□□□ □□□ □□□ □□ □□ □□□ □□□.
C. □□□ □□□ □ AML □□□□□□□ □□□□ □□ □□□ □□□ □□□ □□□□□ □□□ □ □□□.
D. □□□ □□□□ □□□ □□□□ □□□□□ □□□ □ □□□ □□□□ □□□ □□□□□ □ □□□.
Answer: C (LEAVE A REPLY)
According to the ACAMS Study Guide, 6th Edition, page 184, "The decision to close an account should be made in consultation with the institution's legal counsel and AML compliance officer, and in accordance with the institution's policies and procedures." Closing an account may not always be the best option, as it may trigger the customer's suspicion, interfere with law enforcement investigations, or expose the institution to legal risks. Therefore, the institution should carefully weigh the pros and cons of closing an account, and follow its own internal guidelines.
Reference:
ACAMS Study Guide, 6th Edition, page 184
What steps should the institution take? - Exam4Training
Suspicious Transaction Report (STR) / Suspicious Activity Report (SAR) | AML-CFT

NEW QUESTION: 286
□□□ KYC □ □□□□□ □□□ □□ □□ □□ □□□ □□ □□ □□□ □□□ □□□ □□□ □ □□□ □□□□ □□□ □□□□□□.
KYC □ □□□□ □□□ □□ □□□?
A. □□□□□□ □□ □□□(SAR)□ □□□□ □□ □□□□ □□□□□.
B. □□□ □□□ □□□ □□□□ □□□□□.
C. □□ KYC □□□ □□□ □□□ □□ □□□□□ □□□□ □□ □□□ □□ □□□□□.
D. KYC □□ □□□□□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□ □□□ □□□□ □ □□ □□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
Regular KYC reviews ensure that high-risk customers are monitored for potential changes in their risk profile.
Option D (Correct): The KYC manager must determine why the required review was missed and implement corrective measures to prevent future failures.
Option A (Incorrect): A missed review does not necessarily indicate suspicious activity, so filing a SAR at this stage is not appropriate.
Option B (Incorrect): Removing a customer from the high-risk list without reassessment is a compliance violation.
Option C (Incorrect): Suspending account access without due process may be legally questionable.
Best Practices for KYC Compliance Management:
Ensure automated KYC review tracking to avoid missed reviews.
Conduct risk-based periodic reviews on high-risk customers.
Implement escalation protocols for overdue KYC reviews.
Reference:
FATF Recommendation 10 (Customer Due Diligence)
6th EU AML Directive (6AMLD) on Periodic KYC Reviews
Wolfsberg Group Guidance on KYC Risk Management

NEW QUESTION: 287
□□□ □□□□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□ □□ □□ □□
B. □□□□□ □□ □□□ □□□ □□□ □

C. □□ □□□ □□ □□□ □□ □□ □□□ □□ □□
D. □□□□□ □□□□□ □□□□□ □□□□□ □
Answer: (SHOW ANSWER)
According to the FATF Recommendations, the international standard for anti-money laundering and counter-terrorist financing, beneficial owners are the natural persons who ultimately own or control a customer or the natural persons on whose behalf a transaction is being conducted1 The beneficial ownership criterion is not based on the legal title or the nominal ownership of the funds, but on the effective control or the ultimate entitlement to the funds. Therefore, having signature authority over the account, being the person in whose name an account is opened, or being a trusted party in a correspondent banking relationship are not sufficient to determine the beneficial ownership of funds. These may be indicators of legal ownership or nominee arrangements, but they do not necessarily reflect the true ownership or control of the funds. The most effective criterion for determining the beneficial ownership of funds is having control over such funds or entitlement to such funds, either directly or indirectly, through ownership, voting rights, contractual agreements, trusts, or other means2345 Reference:
1: FATF Recommendations, 2012, Recommendation 10 and Interpretive Note
2: Beneficial Ownership Meaning and Regulation, Investopedia, 2022
3: Ultimate Beneficial Ownership: Understanding Where The Money Comes From, ComplyAdvantage, 2022
4: Beneficial ownership and Irish investment funds, A&L Goodbody, 2021
5: Asset Management and Investment Funds Legal and Regulatory Update, Arthur Cox, 2020

NEW QUESTION: 288
□□ □ □□ □□(EU)□ □□ □□ □□ □□□ □□□□ □□ □□ AML □□□ □□□□□? (2 □□ □□□□□.)
A. □□ □□□ □□ □□□□ □□ □□□ □□□□□.
B. □□□□□ □□□ □□(PEP)□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□□ □□□□□.
D. □□□ □□□ □□□ □□□□□.
E. □□ □□□ □□ □□ □□□ □□□ □□.
Answer: A,D (LEAVE A REPLY)
Asset management companies handle large amounts of funds, making them prime targets for money launderers.
Option A (Correct): Negative news (adverse media) screening is essential for identifying potential financial crime risks.
Option D (Correct): Understanding the source and origin of assets ensures that funds come from legitimate sources.
Option B (Incorrect): PEPs should not be automatically rejected, but enhanced due diligence (EDD) is required.
Option C (Incorrect): While onboarding interviews help, they are not a mandatory AML measure.

Option E (Incorrect): Financial stability reports are useful, but not directly linked to AML compliance.
AML Risks in Asset Management:
High-value transactions that may mask illicit wealth.
Layering through investment portfolios to hide the origin of funds.
Use of offshore structures to evade regulatory scrutiny.
Best Practices for AML in Asset Management:
Conduct enhanced due diligence (EDD) on high-net-worth clients.
Monitor large and unusual transactions.
Screen customers against PEP, sanction, and adverse media databases.
Reference:
FATF Recommendation 22 (AML for Asset Management)
6th EU Anti-Money Laundering Directive (6AMLD)
Wolfsberg Group Asset Management AML Framework

NEW QUESTION: 289
□□□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□□ □□□□□□ 1,200□ □□□ □□□ □□□ □□□ □□□□□. □□ □□□ 10□ □□ □□□□ 5□□ □□□ □□□ □□.
□□□□ □□□ □□□ □□ □□□□□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□ □ □□□□. □□□ □□ □□□□ □□□ □□□□.
□ □□ □□ □□ □□ □□□ □□□□□? (2□□ □□□□□.)
A. □□□ □□ □□□ □□□□□□.
B. □□□□□ □□□ □□□ □□ □□□ □□□□□.
C. □ □□□ 10□ □□ □□□ □ □ □□ □□□□□.
D. □□ □□□□ □□□□ □□□ □□□□□.
E. □□ □□□ □□ □□□□ □□□□□ □□□□.
Answer: D,E (LEAVE A REPLY)
The payment received from an account in an offshore jurisdiction and the lack of beneficial ownership details for the originating account are two money laundering red flags. Offshore jurisdictions are often used by money launderers to hide the source and destination of their funds, as they typically have low transparency and weak regulatory oversight. The absence of beneficial ownership information makes it difficult to identify the true owners and controllers of the funds, and to assess the legitimacy and risk of the transaction. These factors increase the possibility that the payment is related to money laundering, tax evasion, or other illicit activities.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, page 33
ACAMS CAMS Certification Exam Outline, 6th Edition, Domain 1, Task 1.2
ACAMS CAMS Certification Video Training Course, Module 1, Lesson 1.2
Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition), Question 315

NEW QUESTION: 290

□□□ □□□□□ □□□□□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□.

A. □□ □□ □□ □□□ □□□□ □□□ □□□□.

B. □□ □□□□□ □□□□.

C. □□□□ □□□□□.

D. □□□□ □□□□□ □□□□□.

Answer: D (LEAVE A REPLY)

According to the guidance issued by FinCEN and the Federal banking agencies, when a financial institution receives a request for SAR supporting documentation from FinCEN or an appropriate law enforcement or supervisory agency, it must first verify that the requestor is, in fact, a representative of such an agency. This is to ensure the confidentiality and security of the SAR information and to prevent unauthorized disclosures. A financial institution should have procedures for such verification in its BSA/AML compliance program, which may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

Reference:

1: This web page explains the BSA requirement that financial institutions provide SAR supporting documentation in response to requests by FinCEN and appropriate law enforcement or supervisory agencies, and the need to verify the requestor's identity.

2: This document provides answers to frequently asked questions regarding SARs and other AML considerations, including the question of how to handle "keep open" requests from law enforcement.

NEW QUESTION: 291

USA PATRIOT Act□ □□(□□) □□ □□□ □□ □□□ □□□ □□ □ □□□□□□ □□ □□ □ □□□□□ □□□□□.

□□ □ □□□ □ □□ □□□ □□□ □ □□□ □□ □□□□□ □□□□ □□ □ □□ □□□ □□□□□? (2□□ □□□□□.)

A. □□□ □□□ □□□□ □□ □ □□□ □□□ □□

B. □□ □□ 25% □□□ □□□ □□ □□□ □□□□ □□ □ □□

C. □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□□ □□ □□□□ □□

D. □□□ □□ □□ □□ □□□□ □□ □□□ □□ □□□□ □□ □ □□

Answer: A,D (LEAVE A REPLY)

According to Section 313 of the USA PATRIOT Act, U.S. financial institutions are prohibited from maintaining correspondent accounts for foreign shell banks, which are banks that have no physical presence in any country and are not affiliated with a regulated financial group. Therefore, a non-U.S. bank must provide the name and address of all shell banks that it maintains accounts for, if any, to its U.S. correspondent. This is to ensure that the U.S. financial institution does not indirectly provide services to shell banks, which pose a high risk of money laundering and terrorist financing.

According to Section 319 (b) of the USA PATRIOT Act, U.S. financial institutions that provide a correspondent account to a foreign bank must maintain records of the owners of the foreign bank and the name and address of a U.S. person who is authorized to receive service of legal process for records regarding the correspondent account. This is to facilitate the access of U.S. law enforcement authorities to information related to the correspondent account in case of an investigation or a subpoena.

The other two options, B and C, are not required by the USA PATRIOT Act, although they may be part of the due diligence or enhanced due diligence procedures that U.S. financial institutions apply to their foreign correspondent accounts, as per Section 312 of the USA PATRIOT Act.

Reference:

USA PATRIOT Act

FACT SHEET for Section 312 of the USA PATRIOT Act Final Regulation and Notice of Proposed Rulemaking US PATRIOT ACT CAMS Exam: USA PATRIOT Act Requirements for Opening a Correspondent Account

NEW QUESTION: 292

□□ □□ □□□ □□□ □□ □ □□□ □□□□. 3□□ □□□ □□□□□

A. □□ □ □□ □□ □ □□

B. □□□ □□□ □□ □□ □ □□ □□

C. □□ □□□ □□ □□ □□ □□ □□

D. □□ □□ □□

Answer: (SHOW ANSWER)

The Office of Foreign Assets Control (OFAC) is a department of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals1. OFAC regulations cover all persons and entities within the U.S., all U.S.-domiciled entities and their foreign branches, and all U.S. citizens, wherever located or employed2. These include U.S. banks, U.S. corporations, U.S. subsidiaries of foreign corporations, U.S. residents, and U.S. citizens living or traveling abroad3. OFAC regulations do not cover foreign-based entities that have U.S. customers, unless they are owned or controlled by U.S. persons or entities4.

NEW QUESTION: 293

□□ □□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □ □□ □□□ □□ □□□ □□□ □ □□□ □□□?

A. □□□ □□ □□ □□ □ □□□□□.

B. □□ □□□ □□ □□□ □□

C. □□□□ □□□□□ □□□ □□□□□.

D. □□□□□ □□□□ □□

Answer: C (LEAVE A REPLY)

According to the ACAMS study guide, one of the best practices for dealing with law enforcement inquiries is to verify the identity and authority of the law enforcement officer before providing any

information (p. 224). This is to ensure that the inquiry is legitimate and not a phishing attempt or a breach of confidentiality. The compliance officer should also document the inquiry and the information provided, and consult with legal counsel if necessary. The other options are not appropriate, as they may either violate the law, compromise the investigation, or create unnecessary work.
Reference:
ACAMS. (2020). Study Guide for the Certification Examination for Anti-Money Laundering Specialists (6th ed.). Miami, FL: ACAMS.
What Is An AML Officer1
Bank Secrecy Act/Anti-Money Laundering: Requests by Law Enforcement for Financial Institutions to Maintain Accounts 2

NEW QUESTION: 294
□□□□ □ □□□□□□□□ □□□ □□□ □□□ □□□ □□ □□□□□□ □□□□ □□□ □□, □ □□ □□□(□□ □□)□ □□□ □□□ □□□.
A. □□ □□□ □□□□ □□ 12□□□ □ □ □□ AML □□□ □□□□□.
B. □□□ □□□□□□□ □□□□□ □□□□□ □□□□□.
C. □□ □□ □ □□ □□□ □□□□□ □□ □□ □□ □□ □□ □□□ □□□□□ □□ □□□ □ □□□ □□□ □□□□□□ □□□□□.
D. AML □□□□□□ □□ □□□ □□□□□ □□ □□□ □□ □□□□□.
Answer: B (LEAVE A REPLY)
The third line of defense (internal audit) provides independent oversight of an institution's AML/CFT compliance framework.
Option B (Correct): The internal audit function should report to the board's audit committee to maintain independence and objectivity.
Option A (Incorrect): While frequent audits are essential, AML audits should be risk-based rather than mandated at a strict 12-month interval.
Option C (Incorrect): Internal audit must assess remediation plans to ensure they adequately address AML deficiencies.
Option D (Incorrect): The third line of defense should not be involved in daily AML operations to avoid conflicts of interest.
Three Lines of Defense in AML Risk Management:

Line of Defense	Function	Key Responsibilities
First Line	Business Units	Implement risk controls in daily operations.
Second Line	Compliance & Risk Teams	Monitor AML/CFT compliance.
Third Line	Internal Audit	Provide independent assessment of AML controls.

Best Practices for AML Audit Function:
Ensure complete independence from AML operations.
Conduct risk-based audits tailored to emerging threats.

Report audit findings to the board for effective oversight.
Reference:
Basel Committee's "Sound Management of ML/TF Risks"
FATF Recommendation 18 (AML Internal Controls & Oversight)
Wolfsberg Group AML Audit Guidelines

NEW QUESTION: 295

□□ □□□□□□□□□ "□□□□ □ □□□□□□□□ □□□ □□□ □□□ □□"□ □□ □□□ □□□ □□□□□□□. □□□ □□□□□ □□□□□ □□ □□□□□ □□□ □□□ □□□□□□. (□ □ □ □□)

A. □□□ □□ □□□□□ □□ □□□ □□ □□□ □□□ □□□□□□.
B. □□ □□□ □□□□□ □□□□□ □□ □□□ □□□□□ □□□□□ □□□□□ □□□ □□□ □□ □ □□□□□ □□ □□□□□□.
C. □□, □□ □□□ □ □□□□ □□□□□ □□□ □ □□ □□ □□□ □□□□□ □□□□□ □□ □ □□ □□□ □□□□□□.
D. □□ □□□□□ □□□ □□ □□□ □□□□□□□ □□□ □□□ □□□□□□.
E. □□ □□□ □□ □ □□□□□ □□ □□ □□□ □□□□□ □□□ □□□ □□□□□□.

Answer: A,C (LEAVE A REPLY)

The Basel Committee's AML guidelines emphasize risk-based customer due diligence (CDD) and beneficial ownership transparency.
Option A (Correct): CDD policies must be risk-based to apply enhanced due diligence (EDD) for high-risk customers and simplified due diligence (SDD) for low-risk customers.
Option C (Correct): Banks must verify the identity of customers and beneficial owners to prevent financial crime risks.
Why Other Options Are Incorrect:
Option B (Incorrect): Numbered accounts are not strictly prohibited but require strict transparency and due diligence measures.
Option D (Incorrect): CDD procedures must be risk-based, not uniform across all customers.
Option E (Incorrect): Transactions should not be processed until full due diligence is completed, except in rare cases where regulatory exceptions apply.
Best Practices for Risk-Based Customer Due Diligence:
Apply EDD for high-risk entities (e.g., PEPs, offshore companies).
Ensure full beneficial ownership transparency.
Implement ongoing transaction monitoring for risk assessment.
Reference:
Basel Committee's "Sound Management of ML/TF Risks"
FATF Recommendation 10 (Customer Due Diligence)
6th EU AML Directive (6AMLD) on Beneficial Ownership Transparency

NEW QUESTION: 296

□□ □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□□. □□ □□□□ □□ OFAC(□□□□□□□□) □□ □□ □□ □ □□□ □□□ □□□□ □□□ □□□□□. □□□ □ □□ □□ □□□ □□□ □□□?

A. OFAC□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□ □□ □□□ □□□□ □.

B. □□□ □□□ □□□□ OFAC□ □□□□□.

C. □□□ □□□□ □□□□ □□ □□ □□□ □□□ □□□□□ □□□□□.

D. □□ □□□ □□□□ □□□□ □□□ □□ □□□□□.

Answer: B (LEAVE A REPLY)

The Belgian bank should freeze the assets of the customer and report to OFAC, as this is the required action for any US person or entity, or any person or entity within the US, that holds or controls property or interests in property of a person or entity on the OFAC Specially Designated Nationals and Blocked Persons List (SDN List). The SDN List is a list of individuals and entities that are subject to US sanctions and whose assets are blocked by OFAC. The Belgian bank, by maintaining a branch in New York, is subject to the jurisdiction and authority of OFAC, and must comply with its regulations and directives. Allowing transactions, closing the account, or continuing business as usual would violate the sanctions and expose the bank to civil and criminal penalties.

Reference:

ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 6, Section 6.2.1, p. 1691 ACAMS CAMS Certification Exam Outline, 6th Edition, Domain 3, Task 3.1, p. 62 OFAC FAQs: Sanctions Compliance, Question 973 OFAC FAQs: General Questions, Question 84

NEW QUESTION: 297

Egmont Group□ □□ □□□ □□□□□? (2□□ □□□□□.)

A. □□□ □□□ □□ □□ □□ □□

B. AML □□ □□□ □□□ □□□ □□ □□□ □□

C. □□□ □□ □□□ □□□ □□ □□ □□

D. □□□ □□□ □□ □□ □□

E. □ □□ □□ □□ □□□ □□ □□ □□

Answer: A,E (LEAVE A REPLY)

The Egmont Group is an international body of Financial Intelligence Units (FIUs) from around the world. Its primary purpose is to serve as a forum for FIUs to exchange information, and it also sets international standards for AML/CFT measures. Additionally, the Egmont Group does not serve as a prudential regulator for global financial institutions or as an authoritative body in the field of anti-corruption.

NEW QUESTION: 298

□□□ □□□ AML □□□ □□□ □□ □□□ □□□□□? (3□□ □□□□□.)

A. □□□□

B. □□ □□ □□

C. □□ □□ □□
D. □□□
E. □□ □□□
F. AML/□□ □□ □□□
Answer: (SHOW ANSWER)
1. Information Technology Staff: These employees handle systems, databases, and software used for transaction monitoring, customer due diligence (CDD), and other AML processes. They need to understand how to configure and maintain AML systems, recognize suspicious patterns, and ensure data security.
2. Customer Facing Staff: Frontline employees, such as tellers, relationship managers, and customer service representatives, interact directly with customers. They play a crucial role in identifying red flags, conducting enhanced due diligence (EDD), and reporting suspicious activities. Training helps them recognize unusual behavior and follow proper procedures.
3. AML/Compliance Staff: These professionals are directly responsible for AML program management, policy development, and regulatory compliance. They need in-depth knowledge of AML laws, regulations, and best practices. Training ensures they stay updated and can effectively implement AML controls.
Reference:
1. Financial Crime Academy: Ensuring Compliance - Building an Effective AML Training Program
2. ACAMS: AML Training - Preparing Auditors to Adequately Assess AML Programs
3. Financial Crime Academy: AML Training for High-Level Executives
4. Financial Crime Academy: Senior Management AML Training Workshops

NEW QUESTION: 299
□□□□ □□□ □□□□□□□(FIU)□ □□□ FIU□ □□□ □□ □□□ □□□ □ □□□ □□ □ □□□. (□ □□□ □□□□□.)
A. FIU □□ □□□ □□□ □□□□□.
B. □□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
C. □□□□ □ □□□□□□ □□□ □□ □□□ □□□ □□□□ □□□□□.
D. □□□□□ □□□□□□□ □□□ □□□□□ □□□□ □□ □□□ □□□□□.
E. □□ □ □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The Egmont Group is an international network of Financial Intelligence Units (FIUs) that enhances cooperation and information sharing to combat financial crime.
Option A (Correct): The Egmont Group improves global cooperation by enabling FIUs to exchange financial intelligence securely.
Option C (Correct): The group facilitates secure communication channels for sharing money laundering and terrorist financing intelligence.
Option E (Correct): The Egmont Group fosters trust between FIUs, allowing them to work collaboratively on cross-border investigations.
Why Other Options Are Incorrect:

Option B (Incorrect): The Egmont Group does not negotiate case-by-case memoranda of understanding (MoUs) for individual cases.
Option D (Incorrect): The Egmont Group does not draft AML legislation; it provides guidance but does not have regulatory authority.
Key Functions of the Egmont Group:
Facilitating cross-border cooperation among FIUs.
Providing a secure network (Egmont Secure Web) for intelligence sharing.
Developing best practices for AML/CFT investigations.
Reference:
FATF Recommendation 29 (Role of FIUs in AML/CFT)
Egmont Group Charter and Principles for FIU Collaboration
Wolfsberg Group AML Guidance on FIU Information Exchange

NEW QUESTION: 300
Egmont Group of Financial Intelligence Units(Fills)□ □□ □□□ □□ □□□ □□ □□□□□□ □□□□ □□ FIU □□ □□□ □□□□□□ □□ □□□ □□□? (2□□ □□□□□□.)
A. □□□ □□ □□□ □□□ □□□ □□ FIU □□ □□□□ □□ □□□ □□□□□□.
B. □□ □□□ □□ □□ □□□□□ □□ □□ □□ □□□□□□□ □□□□□□ □□□.
C. FIU □□□ □□ □□□ □□□□ □□ □□□□□□ □□□.
D. □□□□ Egmont □□ □□ □□ □□□ □□ FIU□ □□ □□□ □□□□□□.
E. FIU□ □□□□□□ □□□□□□ □□□ □□□ □□□□.
Answer: B,E (LEAVE A REPLY)
The principles of the Egmont Group of Financial Intelligence Units (FILLs) aimed at maximizing cooperation between FILLs to more effectively combat money laundering are [1]:
B . Information exchange should take place informally, without too many formal prerequisites.
(CAMS Manual, 6th Edition, Page 55)

NEW QUESTION: 301
□□□□□□□(FATF) □□□□ □□□, □□ □□(FI)□ □□□□□□□□(SAR)□ □□□□ □□ □□□ □□□□□?
A. □□□□□□ □□ □□ □□(CDD) □□□ □□□ □ □□□□.
B. □□□ □□□□ □□□□□□ □□□ □□(PEP)□□□.
C. □□□□□□ □□□□ □□□□□□ □□□ □□□ □□□□□.
D. □□□□ □□□□□□□ □□ □□□ □□□ □□□□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
A Suspicious Activity Report (SAR) is required when a financial institution detects activity that raises suspicion of money laundering, terrorist financing, or fraud.
Option A (Correct): Inability to verify customer identification documents is a red flag for potential financial crime and may require reporting to the Financial Intelligence Unit (FIU).
Option B (Incorrect): PEPs require enhanced due diligence (EDD), but their involvement alone does not automatically trigger a SAR.

Option C (Incorrect): Dealers in precious metals/stones are high-risk, but being in this industry alone does not warrant an automatic SAR.
Option D (Incorrect): Crypto-to-fiat transactions are not inherently suspicious, but they require monitoring for unusual activity.
Key SAR Filing Triggers:
Transactions that do not match the customer's expected activity.
Incomplete, fraudulent, or unverifiable customer identification.
Use of shell companies or unusual intermediaries.
Large or structured transactions with no apparent legitimate purpose.
Best Practices for SAR Compliance:
Implement robust customer due diligence (CDD) processes.
Monitor transaction behavior against expected patterns.
Follow jurisdictional SAR filing deadlines to avoid penalties.
Reference:
FATF Recommendation 20 (Reporting Suspicious Transactions)
6th EU AML Directive (6AMLD) on Suspicious Transactions Reporting
FinCEN SAR Filing Guidelines

NEW QUESTION: 302
□□ A□ □□ A□ □□□□.
□□ B□ □□□ □□ B□□□□□ □□ □□□ □□ A□ □□ □□□□, □□□ □□□ □□ C□ □ □□ □□ C□ □□□□ □□□□□.
□□ A□□ □□ □□□ □□□□□□ □□□ □□□□□.
A□□□ □□□□□□ □□□ □□□□□ □□□□□ □□□?
A. □□ A□□□ □□
B. □□ A□ □□ B
C. B□□□□□□ □□
D. □□ C□ □□ C
Answer: A (LEAVE A REPLY)
According to the CAMS Certification Package - 6th Edition1, a financial institution that processes a wire transfer is required to file a suspicious transaction report (STR) in the jurisdiction where it is located, if it detects any red flags or indicators of money laundering, terrorism financing, or other financial crimes. The financial institution does not need to file an STR in the jurisdictions of the

originator or the beneficiary of the wire transfer, unless it has a branch or a subsidiary there.
Therefore, the correct answer is A. The transaction in Country A.
Reference:
CAMS Certification Package - 6th Edition1, Chapter 4: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Section: Wire Transfers, pp. 161-162.

NEW QUESTION: 303
□□□□□ □□□ □□□□□ □□ □□□□□ □□ □□ □□□□ □□□?
A. □□ □□□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□
B. □□□□ □ □□□ □□ □□ □□
C. □□□□□□□ □□□□ □□ □□□ □□□ □□□□ □□ □□
D. □□□ □□ □□ □□□□ □□
Answer: D (LEAVE A REPLY)
Implementing a sound customer due diligence (CDD) program is the most effective way to prevent money laundering through financial institutions, according to experts. CDD is the process of identifying and verifying the identity of customers and assessing their risk profile, source of funds, and expected activity. CDD helps financial institutions to detect and prevent money laundering by enabling them to know their customers, monitor their transactions, and report any suspicious or unusual behavior. CDD is also a key requirement of the international standards and best practices for anti-money laundering and combating the financing of terrorism (AML/CFT), such as the Financial Action Task Force (FATF) Recommendations and the Basel Committee on Banking Supervision (BCBS) Guidelines.
The other options are not as effective as CDD, as they are either too narrow or too broad in scope. Ensuring that transaction monitoring systems can identify terrorist financing is important, but it does not address the broader issue of money laundering, which may involve other types of criminal proceeds or activities. Collecting information on beneficial owners and foreign customers is a part of CDD, but it is not sufficient by itself, as it does not cover the risk assessment and ongoing monitoring aspects of CDD. Instituting a policy prohibiting the acceptance of funds intended for terrorist financing is a good practice, but it is not a preventive measure, as it relies on the assumption that the funds are already identified as such, which may not be the case.
Reference:
Customer Due Diligence - FATF-GAFI.ORG
Sound management of risks related to money laundering and financing of terrorism - Bank for International Settlements CAMS Study Guide 6th Edition, page 36-37.

NEW QUESTION: 304
SAR/STR □□ □ □□□ □□ □□□ □□ □□□□ □□□□ □□ □□ □□□□□?
A. □□ □□ □□ □□□ SAR/STR□ □□□ □□ □□ □□.
B. □□ □□ □□ □□□ SAR/STR□ □□ □□ □□□□□□.
C. □□ □□ □□ □□□ SAR/STR□ □□□ □□ □□ □□□ □□□□□.

D. □□ □□ □□ □□□ □□ SAR/STR □□.

Answer: (SHOW ANSWER)

The board of directors or designated specialized committee should be provided with statistical data regarding SARs/STRs filed during the reported period, such as the number, type, value, and geographic distribution of the reports, as well as any trends or patterns identified. This information helps the board or committee to oversee the effectiveness of the firm's AML program, assess the level of compliance risk, and allocate appropriate resources and training. Providing all possible details, names of customers, or copies of SARs/STRs may compromise the confidentiality of the reports, violate data protection laws, or expose the firm to legal liability.

Reference:

ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (6th Edition), Chapter 5, Section 5.3.2, page 223.

The Role of the Money Laundering Reporting Officer - ICAEW, page 14.

NEW QUESTION: 305

□□ □□(FI)□ □□□ □□□□□□ □□□□□ □□□□□ □□ □□ □□ □□□ □□ □□□ □□ (EDD)□ □□□□□ □□□□. □□□□□□ FI□ □□□□□□ □□□ □□□□□ □□□?

A. EDD□□□ □□□ □□□□□□□□ □□□□□□ □□□□□ □□□□□□.

B. □□□□□ EDD □□□ □□ □□□ □□ □□□ □□□ □□ □□□□□□.

C. □□□□□□□ 50%□ □□ EDD□ □□□□□ □□ □□□□□□.

D. FI□ EDD□ □□ □□ □□ □□ □□□ □□□□□ □□□ □□□□□□.

Answer: D (LEAVE A REPLY)

According to the Anti-Money Laundering Specialist (the 6th edition) study guide, a risk-based approach for EDD means that the FI applies more or less stringent measures depending on the level of risk posed by each client1. This allows the FI to allocate its resources more efficiently and effectively, and to focus on the clients that pose the highest risk of money laundering or terrorist financing2. Applying EDD for every new client, regardless of their risk profile, may not be the best use of the FI's resources, and may not reflect the proportionality and relevance of the EDD measures3.

Reference:

1: CAMS Study Guide, 6th Edition, Chapter 3, Section 3.2, page 69

2: CAMS Study Guide, 6th Edition, Chapter 3, Section 3.3, page 70

3: CAMS Study Guide, 6th Edition, Chapter 3, Section 3.4, page 71

NEW QUESTION: 306

□□□□□ □□□ □□□□□□□ □□ □□□ □□□□□ □□ □□□□□ □□□□□ □□□ □□□□□ □ □□□ □ □□□ □□□ □□ □ □□□□□.

□□□ □□□ □□□ □□□ □□□ □□□□□ □□□. (□ □□□ □□□□□□.)

A. □□ □□□ □□□.

B. □□ □□.

C. □□□□□ □□□□□ □□.

D. □□ □□ □□.

Answer: (SHOW ANSWER)

Gatekeepers (e.g., accountants, auditors, lawyers) play a critical role in detecting financial crime.
Option B (Correct): Corporate clients pose higher money laundering risks due to complex ownership structures and cross-border financial activities.
Option C (Correct): The nature of requested services (e.g., offshore structuring, large cash transactions) can indicate potential money laundering attempts.
Why Other Options Are Incorrect:
Option A (Incorrect): The length of time a client has been with an accounting firm does not necessarily indicate financial crime risk.
Option D (Incorrect): Short-term relationships may be high-risk, but understanding the business type and services requested is more critical.
Red Flags for Money Laundering in Professional Services:
Clients requesting offshore structures for no apparent business reason.
Use of complex trusts or nominee directors to obscure ownership.
Unexplained large transactions moving through legal or accounting firms.
Best Practices for Gatekeepers to Prevent Money Laundering:
Perform Enhanced Due Diligence (EDD) on high-risk clients.
Report unusual financial activity to FIUs.
Follow FATF's DNFBP (Designated Non-Financial Businesses and Professions) AML guidelines.
Reference:
FATF Recommendation 22 (AML Compliance for Accountants and Lawyers)
Wolfsberg Group Guidance on DNFBP AML Risks
EU 6th AML Directive (6AMLD) on DNFBP Risk Management
Final Thoughts:
FIUs play a central role in financial intelligence collection and sharing.
The Egmont Group enables cross-border AML cooperation among FIUs.
Gatekeepers, such as accountants and lawyers, must monitor corporate clients for money laundering risks.

NEW QUESTION: 307

A □□□ □□□□□ □□ □□□ □□ □□□ 500□ □□□ □□ □□□(US) □□□□□□.
WTS(Worldwide Terrorist Syndicate)□ Bank A□ □□ □ □□□ 100□ □□□ □□□□□ □□□□.
□□ □□□ WTS□ □□ □□ □□□ □□□□□□□.
□□ □□ □□□ □□ USA PATRIOT ACT□ □□ □□□ □□ □ □□ □□□ □□□ □□□□□□?

A. A□□□ 500□ □□ □□ □□□ □□ □□
B. A□□□ □□ □ □□□□□ WTS□ 100□ □□ □□□ □□□□□□.
C. A□□□ □□ □□□ □□□□□ 100□ □□ □□
D. WTS□ □□□ □□ □□ A□ □□ □ □□□□□ 500□ □□□ □□□□□□.

Answer: C (LEAVE A REPLY)

This potential action is authorized by Section 319 of the USA PATRIOT ACT, which allows the U.S. government to seize funds from a foreign bank's correspondent account in the U.S. if the foreign bank refuses to cooperate with a request for records relating to an investigation of money laundering or terrorist financing. The U.S. government can seize an amount equal to the funds in the account of the target of the investigation, regardless of whether those funds are actually in the correspondent account. In this case, the U.S. government can seize $1 million from Bank A's correspondent account in the U.S. because Bank A holds $1 million in the account of the WTS, which is the target of the forfeiture action.

The other potential actions are not authorized by the USA PATRIOT ACT or other U.S. laws. The U.S. government cannot seize Bank A's entire $5 million correspondent account in the U.S. because that would exceed the amount in the WTS's account and would violate the principle of proportionality. The U.S. government cannot seize the WTS's $1 million account at the non-U.S. branch of Bank A because that would require the cooperation of the foreign jurisdiction where the branch is located, which may not be forthcoming. The U.S. government cannot seize $5 million from the non-U.S. branch of Bank A where the WTS's account is located because that would also require the cooperation of the foreign jurisdiction and would exceed the amount in the WTS's account.

Reference:

CAMS Certification Package - 6th Edition | ACAMS, Chapter 3: International Standards and Global Initiatives, pp. 67-68 CAMS Certifications: How to Get CAMS Certified | ACAMS, CAMS Study Guide, pp. 54-55 How Does the Patriot Act Affect Criminal Investigations? | Nolo, Section 319: Forfeiture of Funds in United States Interbank Accounts The USA PATRIOT Act at 20: Sneak and Peek Searches - CRS Reports, Section 319: Forfeiture of Funds in United States Interbank Accounts

NEW QUESTION: 308

□□□ □□□ □□□ □□□□□?

A. □□ □□ □ □□ □□ □□ □□

B. □□ □□ □□

C. □□□ □□□□ □□ □□□ □□□□ □□ □□□□□.

D. □□□□ □□□ □□□ □□□□□.

Answer: A,C (LEAVE A REPLY)

Economic sanctions are measures imposed by countries or international bodies to exert pressure on individuals, entities, or nations that engage in undesirable behavior or actions. Sanctions aim to restrict or prohibit certain economic activities with the targeted parties, such as trade, investments, or financial transactions. They serve various purposes, including achieving foreign policy and national security objectives and deterring undesired actions by countries or entities. Sanctions can be comprehensive (affecting an entire country) or targeted (specific businesses, groups, or individuals), with a recent trend toward minimizing harm to innocent civilians12.

Reference:

1. Council on Foreign Relations: What Are Economic Sanctions?
2. [Tookitaki: A Complete Guide to Sanctions](https://www.tookitaki.com/compliance-hub/what

NEW QUESTION: 309
□□□ □□□□□ □□ AML □□□ □□□ □□□□ □□□ □□ □□□/□□□ □□□ □□ □ □□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □ □□ □□
D. □□□ □□ □□ □□
Answer: C ([LEAVE A REPLY]())
Predicate offenses are the criminal activities that generate the proceeds that are later laundered through money laundering schemes. A country that does not have strong predicate offenses and is lax in prosecuting AML cases could suffer from increased organized crime and corruption, as criminals would have more opportunities and incentives to engage in illicit activities and evade detection and punishment. Organized crime and corruption can have serious social and economic consequences for a country, such as undermining the rule of law, eroding public trust, threatening national security, harming human rights, reducing economic growth, and distorting market competition123.
Reference:
CAMS Certification Package - 6th Edition | ACAMS
Understanding Predicate Offences: The Hidden Web of Money Laundering
Predicate Offenses In Money Laundering - Financial Crime Academy
AML Terms Easily Confused: Predicate Offense vs. Money Laundering

NEW QUESTION: 310
□□□□ □□□ □□ □□□ □□□□□?
A. □□□□□□□(Financial Intelligence Unit)□ □□□ □□□ □□□ □□□□ □□□ □□ □□.
B. □□ □□□□□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□ □□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □□.
D. □□ □□□ □ □□ □□□ □□□ □□ □ □□□ □ □□□ □□□□□ □□□ □□□□ □□□ □□ □□ □□□ □□□□□.
Answer: A ([LEAVE A REPLY]())
https://egmontgroup.org/en/content/about
"The Egmont Group is a united body of 165 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). This is especially relevant as FIUs are uniquely positioned to cooperate and support national and international efforts to counter terrorist financing and are the trusted gateway for sharing financial information domestically and

internationally in accordance with global Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) standards.

NEW QUESTION: 311

□□ □□ □□ □□□□ □□□ □□ □□□ □□□ □□ □□□ □□□□□?

A. □□ □□□□ □□□□

B. □□□ □□□□ □□ □□ □□□ □□□□□ □□□□□.

C. □□□□□ □□ □□ □ □□ □□□ □□□□□ □□

D. □□□ □□□□ □□□ □ □□□□□ □□□ □□□ □ □□□□□ □□□□ □□ □ □□□□.

Answer: (SHOW ANSWER)

correspondent agreement

Explanation:

https://www.bis.org/publ/bcbs85.pdf - page 12

Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

NEW QUESTION: 312

□□ □□ □□□ □□□ '□□ □□'□ □□□□□ □□□□ □□ □ □□□ □□□ □ □ □□□□?

A. □□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□□ □□□ □ □□□□.

B. □□□□□□ □□□ □ □□□ □□ □□□ □□□ □ □□□□.

C. □□□□ □□□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□ □3□□□ □□□ □□□ □ □□□□.

D. □□□□ □□□□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□ □□ □3□□□ □□□ □□□ □ □□□□.

Answer: (SHOW ANSWER)

A free-look provision is a period of time, typically 10 to 30 days, in which a new life insurance policy owner can terminate the policy and have their premium refunded1. This can help criminals to launder money by purchasing a policy with illicit funds and then cancelling it within the free-look period to receive a clean check from the insurance company2. This way, they can disguise the source and origin of their funds and avoid any penalties or charges that would otherwise apply to early termination of the policy.

Reference:

1: Investopedia, What Is a Free Look Period and How Does It Work?
2: FinCEN, Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies

NEW QUESTION: 313
□□ □□(FI)□ □□□□□ □□ □□ □□□ □□□□ □□ □□□□ □□ □□□□ □ □□ □□ □□□ □□□□□? (2□□ □□□□□.)
A. □□ □□
B. □□□□ □□
C. □□ □□□
D. □□□□
E. □□□□ □□□□ □□
Answer: ([SHOW ANSWER]())
Sanctions screening and transaction monitoring rules are two of the most common controls that FIs use to identify suspicious money-laundering activity. Sanctions screening is the process of checking customers, transactions, and counterparties against various lists of sanctioned individuals, entities, and countries issued by national and international authorities. Sanctions screening helps FIs to avoid doing business with or facilitating the activities of those who are involved in terrorism, proliferation, human rights violations, or other criminal activities. Transaction monitoring rules are the criteria or scenarios that FIs use to detect unusual or potentially suspicious patterns of transactions or behaviors of customers or accounts. Transaction monitoring rules help FIs to identify transactions that deviate from the expected norms, such as large cash deposits, frequent wire transfers, or transactions with high-risk jurisdictions. Transaction monitoring rules also help FIs to comply with their reporting obligations, such as filing Suspicious Activity Reports (SARs) or Currency Transaction Reports (CTRs).

NEW QUESTION: 314
□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□□ □ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□?
A. □□ □□□ □□ □□□□□.
B. □□ □□ □ □□ □□□ □□.
C. □□□ □□ □□□ □□□□□.
D. □□□□ □ □□ □□.
Answer: ([SHOW ANSWER]())
A personal banking customer who simultaneously opens several accounts with almost identical names will most likely cause further inquiry, as this could indicate an attempt to evade transaction monitoring, reporting, or identification requirements. For example, a customer could open accounts with slight variations of their name, such as John Smith, Jon Smith, J. Smith, or John Smyth, to avoid detection or aggregation of their transactions. This could also be a sign of identity theft, fraud, or money muling. Therefore, the bank should verify the customer's identity and the purpose of the accounts, and monitor the activity for any suspicious patterns or behaviors.

Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 4, Section 4.2.2, p. 1051 ACAMS CAMS Certification Exam Outline, 6th Edition, Domain 2, Task 2.1, p. 52 FATF Guidance on the Risk-Based Approach for the Banking Sector, October 2014, p. 353

NEW QUESTION: 315
□3□ □□□□ □□□□□□□□ □□□□ 3□ □□□ □□□□□?
A. □□□□
B. □□□
C. □□□
D. □□□ □□□
Answer: A,C,D (LEAVE A REPLY)
The Third European Union Money Laundering Directive (3MLD) is a legal framework that aims to prevent the use of the financial system for the purposes of money laundering and terrorist financing. It was adopted in 2005 and repealed by the Fourth European Union Money Laundering Directive (4MLD) in 2015. The 3MLD applies to a range of entities that are considered to be exposed to the risk of money laundering and terrorist financing, such as:
Financial institutions, which include credit institutions, financial intermediaries, insurance companies, investment firms, and payment service providers.
Casinos, which include both online and offline gambling services that involve wagering a stake with monetary value.
Real estate agents, which include both natural and legal persons that act as intermediaries in the buying and selling of real property or rights over it.
The 3MLD requires these entities to implement a number of measures to prevent and detect money laundering and terrorist financing, such as:
Conducting customer due diligence, which involves identifying and verifying the customer and the beneficial owner, understanding the purpose and nature of the business relationship, and applying enhanced or simplified measures depending on the level of risk.
Keeping records of customer and transaction data for at least five years after the end of the business relationship or the execution of the transaction.
Reporting suspicious transactions or activities to the competent authorities without delay and without tipping off the customer.
Establishing internal policies, procedures, and controls to ensure compliance with the 3MLD, and providing adequate training and awareness to staff.
Cooperating with the relevant supervisory and regulatory authorities and financial intelligence units.
The 3MLD does not apply to defense attorneys, as they are not considered to be obliged entities under the directive. However, the 3MLD does apply to other legal professionals, such as notaries, lawyers, and accountants, when they perform certain activities on behalf of their clients, such as:
Buying and selling of real property or business entities
Managing of client money, securities, or other assets

Opening or managing bank, savings, or securities accounts
Organizing contributions for the creation, operation, or management of companies Creating, operating, or managing trusts, companies, foundations, or similar structures Reference:
THE THIRD EU DIRECTIVE ON MONEY LAUNDERING AND TERRORIST FINANCING, page 11-12 Anti-money laundering and countering the financing of terrorism legislative package, page 1 CAMS Study Guide - 6th Edition, Chapter 1, Section 1.2, page 11 V

NEW QUESTION: 316
□□□□□□ □□ □4□ □□□□□ □□□□□ □□ □□ □□□□ □□□□□ □□□□?
A. □□□□□□ □□□□ □□□□□ □□□□ □□ □□□□□□□ □□□□□□ □□□□□ □□□□ □□□□□ □.
B. □□□ □□□ □□ □□ □□ □□□□□ □□ □□□□ □□□□ □□□□□□ □□□□□□.
C. □□□□□ □□□□ □□□□ □□□□□ □□ □□□□□ □□□□□□ □□□□□□.
D. □□□□□ □□□□□ □□ □□□□ □□ □□ □□□□ □□□□□□ □□□□□□.
Answer: (SHOW ANSWER)
Financial Action Task Force recommendations
Explanation:
The Fourth European Union Directive on money laundering (AMLD4) requires member countries to maintain registries of the beneficial owners of legal entities, such as companies, trusts, foundations, etc. This is to ensure that the true identity and ownership of the customers and the natural persons on whose behalf transactions are conducted are known to the obliged entities, such as banks, lawyers, accountants, etc., and to the competent authorities, such as regulators, supervisors, or law enforcement12. This requirement aims to prevent the misuse of legal entities for money laundering or terrorist financing purposes, and to enhance transparency and access to beneficial ownership information34.

NEW QUESTION: 317
FATF(Financial Action Task Force) □□□ □□ □□□□ □□ □□□□ □□□□□□? (2□□ □□□□ □.)
A. □□ □□□ □□ □□□ □□ □□ □□
B. □□ □□□ □□□ □□ □□ □□
C. FATF □□ □□□ □□ □□□ □ □□ □□
D. □□□ □□□□ □□ □□ □□ □□

E. FATF □□ □□□ □□□□ □□ □□

Answer: C,E (LEAVE A REPLY)

The primary purposes of Financial Action Task Force (FATF)-Style Regional Bodies are to promote effective implementation of FATF recommendations and to provide expertise and input in FATF policy-making. (CAMS Manual, 6th Edition, Page 180)

NEW QUESTION: 318

□□□ □□□ □□□□ □□□□ □□□□. □□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□□□□. □□□□ □ □□□ □□ □□□ □□□ □□□ □□□ □□□□□□.
□□□□□□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□□?

A. □□□ □□□□ □□ □□□ □□□□□□.

B. □□ □□ □□□ □□(Financial Action Task Force) □□□□□ □□ □□□ □□□□□ □□ □□.

C. □□□ □□□ □□□ □□ □□□ □□□□□□.

D. □□□ □□ □ □□ □□□ □□ □□□ □□(□□)□ □□□□□□.

Answer: D (LEAVE A REPLY)

The customer activity that should trigger a suspicious transaction report is purchasing travelers checks (cheques) for trips to a Non-Cooperative Countries and Territories (NCCTs). This could indicate an attempt to evade currency reporting requirements, avoid sanctions or embargoes, or facilitate money laundering or terrorist financing through high-risk jurisdictions12. NCCTs are countries or territories that have been identified by the Financial Action Task Force (FATF) as having serious deficiencies in their anti-money laundering and counter-terrorist financing regimes, and that pose a threat to the international financial system3.

The other options are not necessarily grounds for a suspicious transaction report, although they may require further due diligence or monitoring depending on the customer profile and the nature of the transaction. For example:

The increased activity is due to money order deposits. This could be a legitimate source of income for the customer's export business, or it could be a way of disguising the origin or destination of the funds. The anti-money laundering specialist should verify the identity and background of the customer and the issuers of the money orders, and check for any red flags or suspicious indicators4.

Wire transfers are coming from a Financial Action Task Force member country. This could be a normal business practice, or it could be a sign of involvement in trade-based money laundering or other illicit activities. The anti-money laundering specialist should assess the customer's source of funds, business rationale, and market conditions, and monitor for any changes or inconsistencies.

The client changed his address without advising the institution. This could be a simple oversight, or it could be a way of concealing the customer's true location or identity. The anti-money laundering specialist should update the customer's information, verify the new address, and check for any adverse media or sanctions.

Reference:

ACAMS CAMS Certification Video Training Course - Exam-Labs3

Exam CAMS: Certified Anti-Money Laundering Specialist (the 6th edition)4 ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 1, page 11: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-1.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 2, page 29: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-2.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 4, page 77: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-4.pdf ACAMS Study Guide for the Certification Examination, 6th Edition, Chapter 5, page 97: https://www.acams.org/wp-content/uploads/2019/08/ACAMS-Study-Guide-6th-Edition-Chapter-5.pdf

NEW QUESTION: 319
□□□□□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□?
A. □□□ □□ □ □□□ □□□□ □□ □□ □□ □□□□ □□□□□.
B. □□ □□□ □□ □□□ □□ □□ □□ □□□□ "□□□"□□ □□□□ □□ □□□ □□ □ □□□□□□.
C. □□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□(EDD)□ □□□□□.
D. □□□□□ □ □□□ □□□□ □□□ □□ □ □□□ □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Sanctions compliance is mandatory for financial institutions (FIs) to prevent transactions with sanctioned individuals, entities, and countries.
Option A (Correct): Automatic sanctions screening is essential for detecting and blocking transactions involving sanctioned individuals or entities.
Option B (Incorrect): If a customer is sanctioned, their transactions must be frozen immediately, not just monitored.
Option C (Incorrect): EDD is not relevant for prohibited entities-sanctions require immediate asset freezing.
Option D (Incorrect): Funds must be frozen immediately, without waiting for board approval.
Best Practices for Sanctions Compliance:
Use automated screening tools to detect sanctioned entities.
Immediately block and report prohibited transactions.
Regularly update sanctions screening lists (e.g., OFAC, UN, EU).
Reference:
FATF Recommendation 6 (Targeted Financial Sanctions Compliance)
OFAC Sanctions Guidelines (U.S. Treasury)
EU Sanctions Regulation on AML Compliance

NEW QUESTION: 320
□□□□□ □□□□ □□ □□ □□□□□ □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □ □□□□□□□. □□ □□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □□□□□□. □ □ □□ □□, □□□ □□ □□□ □□ □□□□ □□□ □□ □□□□ □□ □□□ □□□□□ □

□□ □□□ □ □□ □□□ □□□□□□. □□ □ □□ □□□□ □□ □ □□ □□□□ □□□□ □?

A. □□□ □□□□ □ □□□ □□ □□□ □□□ □□□□□.

B. □□□□□ □□ □□□ □□□ □□□□ □□□ □□□□□.

C. □□□ □□□□□ □□□ □□ □□□ □□□□□.

D. □□□□ □□ □□ □□ □□ □□□ □□□□□.

Answer: ([SHOW ANSWER]())

The compliance officer should report the suspicious activity to the Board of Directors, as they are ultimately responsible for the bank's compliance program and oversight. The Board should be informed of the potential conflict of interest and reputational risk involved in the case, as well as the steps taken by the compliance officer to investigate and file the suspicious transaction report. The compliance officer should not prevent the filing of the report, as this would violate the legal obligations of the bank and expose it to regulatory sanctions and penalties. The compliance officer should not ask the Board member to explain the transaction, as this could compromise the integrity and independence of the investigation and the reporting process. The compliance officer should not maintain standard summary statistical reporting to the Board, as this would not adequately address the seriousness and complexity of the case.

Reference:

ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 5, page 1271 ACAMS CAMS Certification Video Training Course, Module 5, Lesson 22 ACAMS CAMS Certification Exam Outline, Domain 5, Task 13

NEW QUESTION: 321

OFAC □□ □□□ □□ □□□ □□□□□? (2□□ □□□□□.)

A. □□ □□□ □□□□ □□□

B. □□ □□□ □□ □□ □□

C. □□ □□□ □□ □□□

D. □□ □□□ □□ □□

E. □□ □□□ □□

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

OFAC-issued regulations apply to all U.S. persons, including U.S. banks, bank holding companies, and non-bank subsidiaries, regardless of where they are located. This means that foreign subsidiaries of U.S. banks and U.S. branches of a foreign bank are also subject to OFAC compliance. However, intermediaries transacting with U.S. banks, foreign banks with U.S. customers, and foreign import-export companies are not necessarily subject to OFAC regulations, unless they are involved in transactions that involve U.S. jurisdiction or U.S. persons.

Reference:

Basic Information on OFAC and Sanctions

OFAC Consolidated Frequently Asked Questions

Office of Foreign Assets Control - Overview

NEW QUESTION: 322

□□ FIU□ □□□ □ □□ □□□ □□ □ FIU□ □□□ □ □□□ □□□□□?

A. Wolfsberg □□□ □□ □□ FIU□ □□ □□□□ □□ □□

B. □□ □□□ □□□□□ □□□□ □□ □□ FIU□ □□□ □□□□□ □□

C. □□ FIU□ □□□ □□□ □□□ □□□ □□□□.

D. □□ FIU□ □□□ □□□□ □□ Egmont Group□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

According to the Egmont Group of Financial Intelligence Units, which is a network of over 160 FIUs that promotes international cooperation and information exchange, FIUs should share information with foreign FIUs spontaneously, without prior request, when they have reasonable grounds to believe that the information is relevant for the receiving FIU1. This principle is also reflected in the FATF Recommendation 40, which states that FIUs should exchange information with other FIUs, especially when this information concerns money laundering, predicate offences, or terrorist financing2. Spontaneous information sharing can enhance the effectiveness of FIUs, as it can help to identify new leads, trends, patterns, or typologies, as well as to prevent or disrupt criminal activities1.

The other options are not consistent with the best practices of FIU information sharing. For example:

In accordance with Wolfsberg guidelines, submit the information to the other FIU in written form. The Wolfsberg Group is an association of 13 global banks that issues guidance and standards on anti-money laundering and counter-terrorist financing. However, the Wolfsberg guidelines are not binding for FIUs, and they do not specify the format or channel of information exchange between FIUs3. Moreover, submitting information in written form may not be the most efficient or secure way of communication, as it may cause delays, errors, or breaches of confidentiality.

Take no action until contacted by the other FIU. This option contradicts the principle of spontaneous information sharing, as it implies that the FIU with the relevant information will wait for a formal request from the other FIU, instead of proactively sharing the information. This may result in missed opportunities, inefficiencies, or failures in detecting or preventing money laundering or terrorist financing.

Request approval from the Egmont Group prior to sharing the information with the other FIU. This option is unnecessary and impractical, as the Egmont Group does not have the authority or the capacity to approve or deny individual information requests or exchanges between FIUs. The Egmont Group provides a platform and a framework for FIU cooperation, but it does not interfere with the operational autonomy or the bilateral relations of its members4.

Reference:

FATF Recommendation 40: Other Forms of International Co-operation

Egmont Group of Financial Intelligence Units Principles for Information Exchange Between Financial Intelligence Units Wolfsberg Group Egmont Group

NEW QUESTION: 323

□□ □□□□ □□□ □□□ □□ □□ □□ □□□ □□ □□□□ □□. □ □□ □□□□ □□□
□□ □□□ □□□□□.
□□□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□ □□□□ □□
B. □□□ □□□□ □□ □□□□ □□□□.
C. □□□ □□□ □□□ □□□ □□□ □□□□□.
D. □□□ □□□□ □□□□ □□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The bank should request a formal letter be submitted to verify the validity of the request, as this is the best practice to ensure compliance with the law and protect customer privacy. The bank should not confirm or deny the existence of a customer relationship, nor provide any information without proper authorization. The bank should also not inform the board of directors before responding to the request, as this could compromise the confidentiality of the investigation or alert the customer.
Reference:
ACAMS CAMS Certification Video Training Course, Module 2: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Section 2.3: Data Protection and Privacy, Slide 10 ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 2: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Page 51

NEW QUESTION: 324
□□□ □□□ □□□ □□□□ □□ □□ □□□□□□ □□ □□□ □□□ □□□ □□□□ □
□ □□□ □□□□. □□□ □□□ □□□□ □□ □□□ □□ □□, □□ □□, □□ □□ □ □□
□□□ □□□ □□□□□. □□ □□ □□□ □□ □□□ □□□ □ □□ □□□□□?
A. □□□
B. □□□□
C. □□□□□□
D. □□□□
Answer: B (LEAVE A REPLY)
Cryptocurrency is a digital or virtual currency that uses cryptography to secure and verify transactions. Cryptocurrencies are decentralized and operate outside the control of any central authority, such as a government or a bank. This makes them attractive for money launderers, who can use them to transfer funds anonymously, quickly, and globally, without leaving a trace or being subject to regulation. Cryptocurrencies pose more risk of money laundering than other sources of money, such as wire transfers, credit cards, or money service businesses, which are subject to more oversight, verification, and reporting requirements.
Reference:
CAMS Study Guide, 6th Edition, Chapter 1, Section 1.9, page 37
CAMS eLearning Course, Module 1, Lesson 9
ACAMS Crypto Hub

NEW QUESTION: 325

□□□□□□ □□□ □□ □□□ □□□ AML □/□□ □□ □□□ □□□□ □ □□□□?

A. □□ □□□□□□ □□ □□□□ □□ □□□ □□ □□ □□□□ □ □□□□□□□□.

B. □□□□□□□ □□ □□□ 10% □□□ □□□□□□ □□□□ □□□ □□□□.

C. □□□□□□ □□□□□□ □□□□ □□□□.

D. □□□□□□ □□ □□ □□ □□□ □□□ □□ □□□□□□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)

Option D (Correct): If a vendor provides services to sanctioned entities or individuals, an organization risks violating OFAC, EU, or UN sanctions laws, potentially leading to fines, legal action, or reputational damage. Engaging in business in a sanctioned region requires strict due diligence and licensing.

Option A (Incorrect): The personal background of an employee is not relevant unless they currently have direct ties to a sanctioned jurisdiction or person.

Option B (Incorrect): A lack of majority ownership does not automatically indicate AML risk; however, organizations should still assess ownership structures for opacity.

Option C (Incorrect): Privately held companies can be transparent if they disclose ownership and operate within compliance standards.

Why This Matters:

Failing to screen vendors for sanctions risks can result in severe penalties, reputational harm, and regulatory scrutiny. OFAC (U.S.), EU, and UN sanctions prohibit business transactions with specific countries, entities, and individuals. Organizations must conduct thorough due diligence to identify and mitigate sanctions risks.

Reference:

OFAC Sanctions Guidelines & Compliance Framework

EU Sanctions Regulations

FATF Recommendation 6 (Targeted Financial Sanctions Related to Terrorism & Proliferation)

NEW QUESTION: 326

□□□ □□ □□□ □□□□ □□ □ □□□ □□□□ □□ □ □□□ □□□□□□□. □□ 6□□ □□ □□ □□□ □□□ □□□□ □□ □□ □ □□□□ □□ □□□□□□□. □□□ □□ □□□ □ □□□ □□□□ □□□ □□□□□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□ □□ □□□□□.

□ □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□□□□?

A. □□ □□

B. □□□ □□□□□□ □□□□

C. □□□□□□ □□ □□□□

D. □□□□□□ □□□ □□ □□□ □□ □□

Answer: (SHOW ANSWER)

According to the ACAMS CAMS Study Guide, one of the methods that attorneys may use to facilitate money laundering is to make payments to third parties on behalf of their clients, using funds from their client accounts. This may obscure the source and destination of the funds, and create a false appearance of legitimate transactions. Therefore, making payment to various people is a red flag for potential money laundering in this situation.

Reference:

ACAMS CAMS Study Guide, 6th Edition, page 117

FATF Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, June 2013, page 341 AML/CFT Red Flags for Lawyers, AML-CFT.net, October 20202

NEW QUESTION: 327

□□□ □□ □ □□□□ □□□ □□□ □□ □□ □□ □□□□ □□ □□ □□□ □□□□□?

A. □□ □□ □□ □□

B. □□ □□ □□ □□

C. □□ □□ □□

D. □□□□ □□□ □□ □□ □ □□

Answer: (SHOW ANSWER)

A Mutual Legal Assistance Treaty (MLAT) is an agreement between two or more countries that allows for the exchange of information and evidence in the investigation and enforcement of criminal laws. MLATs provide a framework for countries to assist each other with investigations, prosecutions, and other legal matters, including the exchange of information, evidence, documents, and testimony. MLATs are commonly used in investigations related to money laundering, terrorism, and other transnational crimes.

NEW QUESTION: 328

□□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□ □ □□ □□ □□ □□□ □□□ □□ □□ □□ □□□ □□□□□?

A. □□□ □□ □ □□□□ □□□

B. □□□ □□□

C. □□□□ AML □□

D. □□□ □□□□ □□

Answer: A (LEAVE A REPLY)

When considering sharing information across the institution or within the same jurisdiction, the key legal issue that poses challenges to sharing customer-related information is data protection and privacy laws. Data protection and privacy laws exist in most countries and can vary significantly from jurisdiction to jurisdiction. These laws place restrictions on how customer data can be used, shared, and stored, and can limit the ability of financial institutions to share customer-related information with each other. Additionally, these laws may also require financial institutions to take additional steps to ensure the protection of customer data.

NEW QUESTION: 329

FATF(Financial Action Task Force) □□ □□ □□□□□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□ □□□.

A. □□□□□□ □□□ □□□ □□□□ FATF□ □□ □ □□□□□□ □□□□□.
B. □□□ □□□ □□□□□ □□□□□ □□ FATF □□□ □□ □□□ □□□ □□□□□□.
C. FATF 40 □□□□□ □□□□□ □□□□□□□ □□□□□ □□ □ □□ □□□ □□□□□□.
D. □□□□□ □□□ FATF □□□□□ □□ □□□ □□□ □□□□□ □□ □□□□□ □□□□□□.
Answer: A (LEAVE A REPLY)
According to the Anti-Money Laundering Specialist (the 6th edition) resources, the FATF mutual evaluation process is a peer review mechanism that assesses the level of compliance of a country with the FATF 40 recommendations and the effectiveness of its anti-money laundering and counter-terrorist financing system. The mutual evaluation report identifies the strengths and weaknesses of the assessed country and provides recommendations for improvement. The assessed country needs to address the shortcomings identified in the report and agree to post-assessment monitoring by FATF, which involves regular follow-up reports and actions to remedy the deficiencies. The other options are not correct, as they do not reflect the FATF mutual evaluation process or the obligations of the assessed country.
Reference:
: ACAMS Study Guide for the Certified Anti-Money Laundering Specialist (the 6th edition), Chapter 4: International Standards and Global Initiatives, page 97.
: FATF, Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, February 2013, updated October 2019, 1.
: FATF, Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations, October 2019, 2.

NEW QUESTION: 330
□□ □□□ □□□ □□□□□□ □□ □□□ □□□□□□. □□□□□ □□ □ □□ □□ □□□□. □□□□ □□ □□ □ □□□□□□□□ □□□□□□□□□ □□ □ □□ □□□ □□□□□□? (2□□ □□□□□□.)
A. □□ □□□ □□ □□□□ □□ □□□ □□□ □ □□□□.
B. □□ □□□ □□ □□□ □□ □□ □□□ □□□ □ □□□□.
C. □□ □□□ □□□ □□□ □□ □□□□□□ □□ □□□ □□□□□ □□□ □□ □□□ □□ □ □□ □□ □□□□.
D. □□□ □□□ □□ □□□ □ □□□ □□ □ □□□□ □□□□.
E. □□ □□□ □□ □□□ □□□ □ □□□□□□ □□ □ □□□□□ □□□□□□.
Answer: A,C (LEAVE A REPLY)
A lack of information about beneficial owners is a red flag for potential money laundering or terrorist financing. It is important to identify who the actual owners of the company are to understand their potential risk exposure.
Confusing details about the proposed business activity and lack of knowledge about the proposed business are also red flags for potential money laundering or terrorist financing. This could indicate that the proposed business activity is not legitimate and is being used to conceal illegal activities.

Therefore, these two observations should be escalated to the compliance officer for further investigation.

NEW QUESTION: 331
□□□ □□□ □□□ □□□ □□□□□. KYC □□ □□□□ □□□ □ □□□ □□ □□□□ □ □□ □□□□ □□ □□□□ □□□□ □□ □□□□□?
A. □□□ □□□ □□ □ □□□ □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□□□.
B. □□□ □□ □□□ □□□ □□□ □□□ □□□□□ □□ □□□□ □□□□.
C. □□□ □□□ □□□□□□□ □□□□ □□□□ □□□□□□□ □□□ □□□□□□.
D. □□□ □□ □□□ □□ □□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The customer's relocation and expansion to different jurisdictions constitutes a triggering event that requires ongoing due diligence on this client, as it may indicate changes in the customer's risk profile, business activities, or beneficial ownership. The bank should update the customer's information, verify the identity and legitimacy of the new entities, and assess the level of money laundering and sanctions risks associated with the new locations12. The other options are not triggering events, as they are either consistent with the customer's normal business operations or do not affect the customer's risk profile.
Reference:
ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 4, page 931
ACAMS CAMS Certification Video Training Course, Module 4, Lesson 22

NEW QUESTION: 332
□□ □□□ □□ □□□ □□ □□□□ □□□□□□. □ □□□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□□□?
A. □□ □□ □□ □□□□ □□□□ □□ □□□ □□□ □□□□□.
B. □□□ □□ □ □□ □□ □□□□ □□ □□ □□ □□□ □□□□□.
C. □ □□□ □□ □□□ □□□□□ □□□□ □□ □□□□ □□ □□ □□□□ □□□□□.
D. □□□□□ □□□ □□ □ □□□□ □□□ □□□ □□□□□.
Answer: A,C (LEAVE A REPLY)
Verified Answer: = A. Collect further customer reference data and determine what must be Comprehensive Detailed = When an existing customer changes its business scope and

jurisdictions, banks need to manage sanctions compliance risk effectively. Here are the steps they should take:

1. Collect Further Customer Reference Data: Obtain updated information about the customer's new business activities, locations, and counterparties. Understand the nature of their transactions and assess the associated risks. Determine what specific data elements need to be screened (e.g., names, addresses, beneficial owners) and establish the appropriate screening frequency.
2. Deploy an Independent Risk-Based Test: Conduct a comprehensive risk assessment tailored to the customer's changes. This assessment should consider factors such as the customer's industry, geographic exposure, and transaction volume. The risk assessment helps identify high-risk areas that require enhanced scrutiny.
3. Screen Directors and Ultimate Beneficial Owners: Perform sanctions screening not only on the customer but also on their directors and ultimate beneficial owners. This ensures that any potential risks associated with these individuals are identified and mitigated.
4. Perform Politically Exposed Person (PEP) and Negative Media Screenings: Continue to screen the customer and related parties against PEP lists and negative media sources. This helps detect any adverse information related to politically exposed individuals or entities.

By following these steps, banks can proactively manage sanctions compliance risk and safeguard their institution's reputation while adhering to regulatory requirements12.

Reference:

1. Protiviti: Sanctions Risk Assessment: A Key Risk Management Tool
2. Moody's: What Businesses Need to Know About Sanctions Compliance

NEW QUESTION: 333

□□□□□□□□□□□ □□□, □□□□□□ AML □□□□□□ □□ □□ □□□□□□□ □□□□□ □□□□ □□□ □□ □ □□□□□ □□ □□ □ □□ □□□?

A. □□ □□ □□□ □□□ □□ □□, □□ □ □□ □□ □□□ □□ CEO□□ □□ □□□□□ □□, □□□ □□□□□ □□□□□ □□□ □□ □□ □□ □□ □□□ □□ □□□□□□ □□□□□ □□□.

B. □□ □□ □□□ □□□□□□ □□□□□□ □□□ □ □□ □□□ □□, □□, □□□ □ □□□□□□□□ □□ □□□□□ □□□ □ □□□□ □□□.

C. □□□□□ □□□ □□ □□ □□ □□□ □□□ □□□ □□ □□□, □□ □□□□□ □□ □□□□□ □□□□□ □□□□□ □□□□□□ □□□□□ □□ □□ □□□ □□□□□ □ □□□□□□ □ □□□.

D. □□□□□ □□ □□ □□□ □□□□□ □□ □□ □□□ □□, □□, □□□□, □□, □□□□□ □□ □□ □□□ □□□□□ □□□.

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

The Basel Committee on Banking Supervision (BCBS) sets global standards for bank governance and states that the Board of Directors plays a critical role in AML oversight.

Option D (Correct): The Board is responsible for:

Establishing and approving the AML compliance function.

Ensuring the compliance function has adequate authority and resources.

Overseeing risk management efforts and policies.
Option A (Incorrect): The Board should be actively involved, not just informed when required.
Option B (Incorrect): The compliance function must have direct access to the Board to ensure independent oversight.
Option C (Incorrect): The Board must be involved in policy establishment for effective compliance management.
Why Board Oversight is Critical:
Ensures effective AML governance and accountability.
Reduces regulatory risks and potential financial penalties.
Strengthens financial institution stability and reputation.
Best Practices for Board Oversight in AML Governance:
Establish independent compliance reporting lines to the Board.
Ensure regular AML risk assessments and policy reviews.
Mandate regular AML training for senior management.
Reference:
Basel Committee on Banking Supervision (BCBS) Corporate Governance Principles FATF Recommendation 18 (Internal Controls and Board Oversight) Wolfsberg Group AML Risk Management Framework

NEW QUESTION: 334
□□ □ □□□ □□□ □□ □□□□□ □□□ □ □□ □□ □□□ □□□□□□? (3□□ □□□□ □.)
A. □□ □□□ □□ □□ □□□ □□□ □□ □□.
B. □□ □□□ □□□□□□ □□□□ □□ □□ □□.
C. □□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□.
D. □□ □□□□ □□□ □□□□□□□(LLC).
E. □□□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□□ □□ □□ □□□□□□.
Answer: A,C,E (LEAVE A REPLY)
Money launderers exploit corporate structures that offer anonymity and reduced transparency.
Option A (Correct): Nominee shareholders and directors can be used to hide true beneficial ownership.
Option C (Correct): Bearer shares allow ownership to transfer anonymously, a major AML risk.
Option E (Correct): Tax haven companies with secrecy laws are frequently used for money laundering.
Option B (Incorrect): A private company without activity does not inherently pose an AML risk.
Option D (Incorrect): LLCs can be transparent if proper KYC and reporting measures are in place.

NEW QUESTION: 335
□□ □□ □□ □□ □□ □□ □□□ □□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□ □ □□ □□□ □□□□□□?
A. □□□□□□□(FIU)

B. FATF
C. □□ □□□
D. □□□□□□□ □□
Answer: (SHOW ANSWER)
An FIU is a central, national agency responsible for receiving, analyzing, and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime and potential financing of terrorism or required by national legislation or regulation1. FIUs play a crucial role in the detection and prevention of money laundering and terrorist financing by collecting, processing, and analyzing financial intelligence and sharing it with domestic and foreign counterparts2. FIUs may have different organizational structures, functions, and legal frameworks, but they all adhere to the international standards and best practices set by the Egmont Group of FIUs3.
Reference:
What We Do | FinCEN.gov
Financial Intelligence Units: An Overview (June 2004) - IMF, page 1
[Egmont Group of Financial Intelligence Units]

NEW QUESTION: 336
□□ □□□ □□□, □□□ □□□ □□□□□ □□□□ □□ □□□□□□?
A. □□□□□□ □□ □□□ □□□ □□ □□□ □□□ □□□□.
B. □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□.
C. □□□□□□□ □□□□□□ □□ □□□ □□ □□□ □□□□ □□□□□□ □□□□ □□ □□□ □□□□□□.
D. □□□□□□ □□□□ □□□□□□ □□□ □□□□ □□□□□□□ □□□ □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)
Money laundering has a significant negative impact on the financial sector by undermining the integrity of financial markets. It distorts asset and commodity prices and leads to the misallocation of resources, which can dampen economic growth. The process also erodes public trust in the financial system and can deter foreign investment.

NEW QUESTION: 337
□□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □□ □□□□□□□□.
□□ □□ □□ □□□ □□ □□□ □□□□ □□□ □□□.
□□□ □□ □□□ □□□ □□□?
A. □□ □□ □□ □□ □□
B. □□□ □□□□ □□ □□□ □□□□.
C. □□ □□□ □□□□ □□□□□□ □□ □□□ □□□□ □□□□.
D. □ □□□ □□□□□□□ □□□ □□□ □□□□□□ □
Answer: B (LEAVE A REPLY)

If an employee of a financial institution is found to have assisted in money laundering or any other criminal activity, the institution should take appropriate disciplinary action and report the employee to the relevant authorities. This is not only a legal obligation, but also a sound compliance practice to protect the institution's reputation and integrity. Disciplining the employee without informing the authorities would be insufficient and potentially expose the institution to further legal risks.
Ignoring the employee's involvement or requiring additional training for all employees would be ineffective and inappropriate responses.
Reference:
ACAMS CAMS Certification Package - 6th Edition, Chapter 5: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), pp. 121-1221
ACAMS CAMS Certification Package - 6th Edition, Chapter 6: AML Compliance Program, pp. 143-1441 ACAMS CAMS Certification Video Training Course, Module 5: Compliance Standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), Lesson 5.2: International Standards and Best Practices2 ACAMS CAMS Certification Video Training Course, Module 6: AML Compliance Program, Lesson 6.4: Internal Controls2

NEW QUESTION: 338
□□□ □□□□ □□ □□ □□ □□ □ □□□□□ □□□□ □□□□ □□□□ □□□ □□□
□ □□□□?
A. □□□□
B. □□ □□□
C. □□□
D. □□□□□
Answer: D (LEAVE A REPLY)
The compliance officer is the person who has the day-to-day responsibility of communicating and reinforcing the established anti-money laundering (AML) compliance culture and program within the organization. The compliance officer is also responsible for overseeing the implementation, maintenance, and improvement of the AML policies, procedures, controls, and training. The compliance officer should have sufficient authority, independence, and resources to perform their duties effectively and report to senior management and the board of directors on the status and effectiveness of the AML program.
Reference:
1, Chapter 4: Designing and Implementing an AML Compliance Program
2, FFIEC BSA/AML Examination Manual, Compliance Program - Overview
3, FinCEN Advisory, Guidance on Promoting a Culture of Compliance

NEW QUESTION: 339
□□ □□(FI)□ AML □□□□□□ □□ □□□ □□□ □□□□□□□(FIU)□ □□ □□□ □□
□□□ □□□ □□□□□. AML □□ □□□□ □□□ □□ □□□?
(2□□ □□□□□.)
A. □□ □□□□ □□ □□□□ □□□□.

B. □□ □□□ □□ FI□ □□□□ □□□ □□□□.
C. □□□ □□□ □□□□ □□ □□ □□□ □□□□□□□□.
D. □□□ □□ □□ □□□□ □□ □□□ □□□□.
E. □□□ □□□ □□ □□□ □ □□ □□ □□□ FIU□ □□□□□□.
Answer: A,C (LEAVE A REPLY)
According to the Certified Anti-Money Laundering Specialist (CAMS) Sixth Edition manual, the AML compliance officer should inform senior leadership and the board of the investigation (page 124) and monitor the progress of the investigation by keeping clear records (page 127). Additionally, the AML compliance officer should provide all information to the FIU as soon as possible to avoid delays (page 126).
According to the CAMS Manual, when a financial institution is being investigated by the financial intelligence unit (FIU), the AML compliance officer should inform senior leadership and the board of the investigation and monitor the progress of the investigation by keeping clear records. The manual states:
"The AML compliance officer should inform senior leadership and the board of any investigations and then monitor the progress of the investigation by keeping clear records of what has been requested and submitted, deadlines and extensions granted, and any findings or reports received. This will allow the financial institution to respond effectively and efficiently to the investigation and take appropriate action if necessary." (CAMS Manual, Section 7.4.1 - Financial Intelligence Units, p. 366)

NEW QUESTION: 340
Financial Action Task Force □□□□ □□ □□□ □□ □ □□ □□□□ □□ □□□ □□ □□ □□ □ □□ □□ □□ □□□ □□□ □□□? (2□□ □□□□□.)
A. □□ □□□ □□□ □□□ □□□□□.
B. □□ □□□ □□ □□□ □□□□□.
C. □□ □□□□ □□□□ □□□ □□□□□.
D. □□ □□□ □□ □□□ □□ □□□ □□□ □□ □□□□□.
Answer: A,B (LEAVE A REPLY)
According to the Anti-Money Laundering Specialist (the 6th edition) study guide, the Financial Action Task Force (FATF) is an inter-governmental body that sets the global standards for anti-money laundering and counter-terrorist financing (AML/CTF). The FATF also monitors the compliance and implementation of its recommendations by its members and other jurisdictions. To enhance its global reach and effectiveness, the FATF works with nine FATF-style regional bodies (FSRBs) that cover different regions of the world. These FSRBs have similar objectives and functions as the FATF, but they also take into account the specific characteristics and challenges of their regions. Two ways that FSRBs influence AML/CTF standards within their respective regions are:
They issue typologies specific to their geographical region. Typologies are reports or studies that analyze the methods, trends, and patterns of money laundering and terrorist financing in a particular sector, industry, or region. FSRBs produce typologies that reflect the regional context

and risks of their members and provide guidance and best practices to address them. For example, the Asia/Pacific Group on Money Laundering (APG) has issued typologies on trade-based money laundering, wildlife trafficking, and virtual assets in the Asia-Pacific region12.
They administer mutual evaluations of participating members. Mutual evaluations are peer reviews that assess the level of compliance and effectiveness of a country's AML/CTF system against the FATF standards. FSRBs conduct mutual evaluations of their members and publish the results and recommendations in detailed reports. These reports help identify the strengths and weaknesses of each country's AML/CTF regime and provide a basis for follow-up actions and technical assistance. For example, the Caribbean Financial Action Task Force (CFATF) has conducted mutual evaluations of its members such as Barbados, Jamaica, and Trinidad and Tobago34.
Reference:
Anti-Money Laundering Specialist (the 6th edition) study guide, page 27 APG website, section on Typologies Anti-Money Laundering Specialist (the 6th edition) study guide, page 28 CFATF website, section on Mutual Evaluations

NEW QUESTION: 341
□□ □□□□□ □□ □□□□ □□ □□□□ □□□□ □□, □□ □□□□ □□□□□□?
A. □□ 319(a)
B. □□ 314(a)
C. □□ 319(b)
D. □□ 314(b)
Answer: A (LEAVE A REPLY)
The USA PATRIOT Act includes provisions allowing the U.S. government to seize assets linked to financial crime, even when held in foreign financial institutions.
Option A (Correct): Section 319(a) of the USA PATRIOT Act provides U.S. regulators with the authority to seize funds deposited in U.S. correspondent accounts of foreign banks if linked to illicit activity.
Option B (Incorrect): Section 314(a) focuses on information sharing between law enforcement and financial institutions.
Option C (Incorrect): Section 319(b) enables U.S. authorities to seize funds linked to foreign correspondent banking accounts, but 319(a) specifically deals with extraterritorial forfeiture.
Option D (Incorrect): Section 314(b) allows financial institutions to voluntarily share AML-related information.
Why This Matters:
Foreign banks using U.S. correspondent accounts can be subject to U.S. jurisdiction.
Helps U.S. law enforcement disrupt global money laundering networks.
Encourages financial institutions to enhance correspondent banking due diligence.
Reference:
USA PATRIOT Act Section 319(a) (Forfeiture of Funds)
FinCEN Guidelines on Correspondent Banking Risks

FATF Recommendation 13 (Correspondent Banking)

NEW QUESTION: 342

AML □□ □□□□□ □□□□ □□ □□□ □□ □□□□□ □□ □□□□□ □□□□□.
□□□□□ □□ □□□□ □□□□ □□□□ □□□□□.

A. □□ □□□□ □□□□ □□□□ □□ □□□□□ □□ □□□□□ □□ □□□□ □□□□□□.

B. □□□□□ □□ □□ □□ □□□□ □□□□□□.

C. □□□□□ □□ □□□□ □□□□□□ □□ □□□□ □□□□□ □□ □□□□ □□□□□□.

D. □□ □□□□ □□ □□ □□□□ □□□□ □□ □□□□ □□□□□□.

Answer: D (LEAVE A REPLY)

AML audit findings must be analyzed and addressed through remedial actions based on root cause analysis.

Option D (Correct): Root cause analysis helps develop effective corrective measures to prevent recurring AML deficiencies.

Option A (Incorrect): Retesting controls may be useful, but addressing deficiencies is more critical.

Option B (Incorrect): While the board oversees compliance, the responsibility for implementing fixes lies with AML teams.

Option C (Incorrect): Audit teams provide findings but do not execute corrective actions.

Best Practices for Addressing AML Audit Findings:

Identify the root cause of AML control failures.

Develop risk-based remediation plans.

Implement and monitor corrective actions.

Reference:

FATF Recommendation 18 (AML Internal Controls & Audit)

Basel Committee's Guidelines on AML Audits

Wolfsberg Group Principles for AML Risk Management

Final Thoughts:

Suspicious stock price movements can indicate market manipulation linked to money laundering.

EU AML and GDPR regulations enforce strict data minimization and AI compliance requirements.

Bearer shares, nominee directors, and tax-haven corporations increase money laundering risks.

AML audit findings should be addressed through root cause analysis and corrective actions.

NEW QUESTION: 343

AML □□□□ □□ □□ □□□□ □□□□□ □□□□ □□□□□ □□□□?

A. □□□□ □□ □□□□□ □□□□□ □□ □

B. □□□□ □□□□□ □

C. □□ □□ □□□□ □□ □

D. □□

Answer: B (LEAVE A REPLY)

New business products should be evaluated for AML concerns before they are launched into the market. This is because new products may introduce new risks or vulnerabilities that could be exploited by money launderers or terrorist financiers. By conducting a pre-launch assessment, a financial institution can identify and mitigate these risks, design appropriate controls and procedures, and ensure compliance with the relevant laws and regulations. A pre-launch assessment can also help a financial institution to align its AML strategy with its business objectives, and avoid potential reputational damage or regulatory sanctions.

Reference:

9 Things to Consider When Evaluating an AML Solution

CAMS Study Guide 6th Edition, page 38.

NEW QUESTION: 344

FIU(Financial Intelligence Units)□ □□□ □□□□□.

A. □□□ □ □□ □□□ □□□ □□□□□.

B. □□ □□□□ □□□ □□□ □□ □ □□ □□□ □□□ □□□□□.

C. □□ FIU□ □□ □□.

D. □□ □ □□ □□□□□□ □□□ □□ □□□ □□□ □□ □.

Answer: A (LEAVE A REPLY)

Financial Intelligence Units (FIUs) are national agencies that collect, analyze, and disseminate information on suspicious or unusual financial activity, such as money laundering and terrorist financing, to relevant authorities. One of their main functions is to disseminate the results of their analysis to law enforcement agencies in a timely manner, so that they can initiate investigations or prosecutions. This is also one of the standards set by the Financial Action Task Force (FATF), the global body that sets the anti-money laundering and counter-terrorist financing (AML/CFT) policies and recommendations. The other options are not the primary responsibilities of FIUs, although they may perform them as part of their mandate or in cooperation with other agencies.

Reference:

What are Financial Intelligence Units (FIUs)? | Dow Jones

Financial Intelligence Units: An Overview - IMF

Financial Intelligence Units - Egmont Group

FATF Recommendation 29 - Financial Intelligence Units (page 17)

NEW QUESTION: 345

□□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?

A. □□

B. □□ □□

C. □□□

D. □□ □□

Answer: B (LEAVE A REPLY)

Cash couriers are individuals who physically transport cash or other monetary instruments across borders or within a country, often to avoid detection by authorities or reporting obligations. Cash

couriers are a common method used by terrorist financiers to move funds without leaving an audit trail, as cash is anonymous, portable, and widely accepted12.
Reference:
1: ACAMS CAMS Certification Video Training Course, Module 4: Terrorist Financing, Section 4.2: Methods of Terrorist Financing, Slide 9 2: ACAMS CAMS Certification Study Guide, 6th Edition, Chapter 4: Terrorist Financing, Page 97
20Typologies%20Report.pdf (24)

NEW QUESTION: 346
□□□ □□□ STR□ □□ □ □□ □□□□□□□ □□ □□□ □□ □□ □□□ □□□ □□ □□ □?
A. STR □□□ □□ □□□ □□□ □□□ □□□ □□□.
B. □□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□.
C. □□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□□ □□ □□□.
D. □□□□□ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□ □□□ □□□ □□□ □.
Answer: A ([LEAVE A REPLY](#))
According to the BSA/AML Manual1, one purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. Therefore, when an institution receives a document request from law enforcement with regard to an STR that the institution has filed, it should cooperate and provide the documents that were previously collected to support the STR. This will help the law enforcement agency to conduct its investigation and follow up on the suspicious activity reported by the institution. The institution should also maintain the confidentiality of the STR and the document request, and avoid tipping off the customer or any other person involved in the suspicious activity.
Reference:
BSA/AML Manual1
Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations2 Suspicious Transaction Report STR3

NEW QUESTION: 347
□□ □ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□□?
A. □□ □□□□ □□ □□ □□□□□ □□ □□(SAR)□ □□□□ □□□ □□□□ □□□□.

B. □□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□□□.
C. □□□ □□ □□ □□(SDN)□ □□□□ □□ □□ □□□ □□□□□.
D. □□□ □□□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Financial institutions must close accounts that violate sanctions laws or pose a severe AML risk.
Option C (Correct): Doing business with Specially Designated Nationals (SDNs) violates U.S. OFAC and EU sanctions, requiring account closure.
Option A (Incorrect): Multiple SARs do not always require account closure; the institution may continue monitoring the customer.
Option B (Incorrect): Tuition payments are normal transactions and do not justify account closure.
Option D (Incorrect): A civil subpoena does not imply financial crime and does not require closure.
Key Account Closure Triggers:
Violation of OFAC, EU, or UN sanctions laws.
Confirmed criminal activity (e.g., fraud, money laundering, terrorist financing).
Regulatory directive or legal requirement to terminate the account.
Best Practices for Account Closure:
Document the justification for closure (e.g., sanctions compliance, AML concerns).
Notify the customer in a manner that does not constitute "tipping off." File SARs where required before closing high-risk accounts.
Reference:
OFAC Sanctions Compliance Guidelines
FATF Recommendation 6 (Targeted Financial Sanctions)
Wolfsberg Group AML Account Closure Best Practices

NEW QUESTION: 348
□□ □□□ □□ Base1 □□□□□ □□□ KYC □□□□□ □□ □□□ □□□□□?
(2□□ □□□□□.)
A. □□ □□
B. □□ □□ □□
C. □□ □□
D. □□ □□
E. □□ □□
Answer: B,E (LEAVE A REPLY)
https://www.bis.org/publ/bcbs110.pdf
According to the Basel Committee on Banking Supervision, a sound KYC program should include four essential elements: customer acceptance policy, customer identification, on-going monitoring of higher risk accounts, and risk management1. Customer acceptance policy defines the types of customers that the financial institution (FI) is willing to accept and the criteria for doing so. Customer identification involves verifying the identity and beneficial ownership of the customers and obtaining information on their activities and sources of funds. On-going monitoring of higher risk accounts involves reviewing the transactions and behavior of the customers that pose higher

risks of money laundering or terrorist financing and updating their information and risk profiles. Risk management involves establishing appropriate policies, procedures, controls, and audit functions to ensure the effective implementation and oversight of the KYC program1.
Reference:
1: Basel Committee on Banking Supervision - Bank for International Settlements1

NEW QUESTION: 349
□ □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□. □□□ □□□□□ □□ □, □□ □□□ □□□□ □□□□ □□□□□ 100□□ □□□ □□□ □ □□□□ □□□ □□ □□□.
□□□□ □□□ □□□ □ □□□ □□ □□□?
A. □□□ □□ □□□ □□
B. □□□ □□ SAR □□
C. □□□ □□□ □□□ □□□□
D. □□□ □□ □□□ □□□ □□ CTR □□
Answer: (SHOW ANSWER)
A customer who is nervous, uneasy, or in a hurry to cash a large cashier's check may be trying to launder money or evade reporting requirements. The teller should complete the transaction as normal, but also flag the customer's account for further monitoring and review. The teller should look for any unusual or suspicious patterns of activity, such as frequent large cash transactions, transfers to or from high-risk jurisdictions, or transactions that do not match the customer's profile or expected behavior. The teller should also document the transaction and the customer's demeanor, and report any findings or concerns to the appropriate authority within the bank.
The teller should not confer with the bank's account going forward, as this may alert the customer to the bank's suspicion or compromise the investigation. The teller should not file a SAR on the customer, unless there are other grounds to suspect money laundering or terrorist financing, as this may be premature or unnecessary. The teller should not file a CTR on the customer by the end of the day, unless the transaction exceeds the threshold of $10,000, as this is a legal requirement for cash transactions in the US.
Reference:
[ACAMS Study Guide for the CAMS Certification Examination, 6th Edition], Chapter 4: Conducting or Supporting the Investigation Process, pp. 103-104, 107-108.
Suspicious Activity Reporting - Overview, Federal Financial Institutions Examination Council, April 2018, pp. 1-2, 4-5.
Currency Transaction Reporting - Overview, Federal Financial Institutions Examination Council, April 2018, pp. 1-2, 4-5.
17 AML Analyst Interview Questions and Answers, CLIMB, July 15, 2022.

NEW QUESTION: 350
Financial Crimes Enforcement Network□ □□□ □□□ □□ □□ □□□□□ □□ □□□□ □ □□ □ □□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□□□ □□□?

A. 30□
B. 60□
C. 90□
D. 120□
Answer: (SHOW ANSWER)
a financial institution must perform a continuing review of the account for a period of 90 days. The continuing review must include an analysis of any transactions that occur in the account, as well as any changes in the customer's risk profile. The review should be updated as needed to ensure that the customer is not engaging in any suspicious activities.

NEW QUESTION: 351
□□ □□ □□ □□□(Basel Committee on Banking Supervision)□ □□□ □□□ □□□ □□ □□□ □□□ □□□□ □□□.
A. □□□ □□ □ □ □□ □□□ □□ □□□ □ □□□ □□□ □□□ □□□□□.
B. □□ □□□ □ □ □□□□□□□ □□ □□ □□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□ □□□□□ □□□□ □□□ □□□ □□□□□.
D. □□□ □□□□ □□ □□□□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
According to the Basel Committee on Banking Supervision, banks should apply a risk-based approach to customer due diligence, which means that they should adopt enhanced measures for higher-risk customers and simplified measures for lower-risk customers. Enhanced due diligence (EDD) may include obtaining additional information on the customer's identity, source of funds, business activities, beneficial owners, and expected transactions, as well as conducting more frequent and intensive monitoring of the account activity. EDD is especially important for customers who are politically exposed persons (PEPs), who are from or have connections with high-risk countries or jurisdictions, or who are involved in high-risk industries or sectors. Therefore, performing EDD including enhanced ongoing monitoring of the account activity is the correct way for banks to deal with high-risk customers.

NEW QUESTION: 352
STR □□□ □□ □□□□ □□□□ □□ □□ □□□□ □□□?
A. □□ □□□ STR□ □□ □□ □ □□□ □□□ □□□.
B. □□□□ □□□ □□ STR□ □□□ □□□□ □□□.
C. □□ STR □□□ □□□□ □□□□ □□□.
D. □□□ □ □□ □□□ □□□ □ □□ □□□ □□ □□□□□ □□□.
Answer: (SHOW ANSWER)
According to the ACAMS CAMS Certification Study Guide (6th edition), senior management and the Board of Directors have the ultimate responsibility for the effectiveness of the AML program and the compliance with the relevant laws and regulations. Therefore, they should be informed of all significant STRs and the numbers and trends of the filings, as this would help them to assess the level of risk exposure and the adequacy of the controls and resources. The other options are

either too restrictive or too burdensome for senior management and the Board of Directors, and may interfere with the timely and confidential filing of STRs.

NEW QUESTION: 353

FATF(Financial Acton Task Force)□ □□□ □□ □□ □□/□□□□ □□□ □□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□□?

A. □□□ □□□ □□□□

B. 1□□ 3□ 2□□ □□ □□□ □□□□

C. FATF □□□□□ □□□ □□□□□□□□ □□□□

D. □□□ □□□□ 4□□ □□ □□□ □□□□

Answer: B (LEAVE A REPLY)

The FATF communicates its findings regarding jurisdictions with strategic AML/CFT deficiencies by issuing two formal documents three times per year, namely the FATF Public Statement and the Improving Global AML/CFT Compliance: On-going Process document1. These documents identify the jurisdictions that have serious and/or systemic deficiencies in their AML/CFT regimes and the progress they have made in addressing them. The FATF also calls on its members and other jurisdictions to apply counter-measures or enhanced due diligence measures to protect the international financial system from the risks emanating from these jurisdictions1.

Reference:

1: High-risk and other monitored jurisdictions - Financial Action Task Force (FATF)

NEW QUESTION: 354

□□ □□(FI)□ □□ □□□□ □□ □ □□ □□□□□□□ □□□ □□ □□ □□□ □□□□□. FI□ □□ □□□ □□□ □□□?

A. □□ □□□ □□□□ □□ FIU(Financial Intelligence Unit)□ □□□ □□□□□.

B. □□ □□□ □□□ □□ □□ □□□ □□□□□.

C. □□□ □□□□ □□□ □□□□ □□□□□.

D. □□□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□□□□□.

Answer: (SHOW ANSWER)

The best course of action for the FI in this scenario is to consider retaining qualified, experienced legal counsel. This is because the investigation request from the local law enforcement agency may involve complex legal issues, such as confidentiality, privacy, data protection, and cooperation obligations. The FI may need to balance the interests of the customer, the law enforcement agency, and the FI itself, and ensure that it complies with the applicable laws and regulations in responding to the request. The legal counsel can advise the FI on the scope, validity, and implications of the request, and help the FI to prepare and submit the required information in a timely and appropriate manner. The legal counsel can also protect the FI from any potential liability or litigation arising from the investigation.

Reference:

1: Requests by Law Enforcement for Financial Institutions to Maintain Accounts and/or Conduct Transactions1

2: Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations2
3: ACAMS Study Guide for the CAMS Certification Examination3