DUMPSBOSS.

Certified Anti-Money Laundering Specialist (6th Edition)

ACAMS CAMS

Version Demo

Total Demo Questions: 58

Total Premium Questions: 583

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Risks and Methods of Money Laundering and Terrorist Financing	131
Topic 2, Compliance Standards for Anti-Money Laundering and Combating the Financing of Terrorism	198
Topic 3, Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Compliance Programs	133
Topic 4, Conducting or Supporting the Investigation Process	121
Total	583

QUESTION NO: 1

What might limit a compliance officer's ability to respond to a foreign law enforcement official's request to provide information with regard to an anti-money laundering investigation?

A. Privacy and data protection laws in the compliance officer's country

B. Whether there is a mutual legal assistance treaty between the countries of the compliance officer and the law enforcement official

C. Whether the request has been processed by the foreign law enforcement official's embassy in the compliance officer's country

D. Anti-money laundering laws that require the confidential treatment of Suspicious Transaction Reports in the law enforcement official's country

ANSWER: B

Explanation:

The key limiter is whether there is a mutual legal assistance treaty between the countries of the compliance officer and the law enforcement official. In practice, a foreign law enforcement request often needs to come through formal government-to-government channels (typically via an MLAT request, letters rogatory, or another recognized international cooperation mechanism) before a financial institution can lawfully disclose non-public customer information. Even when a compliance officer wants to assist, the institution generally must ensure there is a valid legal basis to share information cross-border, that the request is properly authorized, and that disclosure is permitted under local banking secrecy, confidentiality, and procedural laws. MLAT frameworks help establish that legal basis and define the scope, process, and safeguards for exchanging evidence and financial records for criminal matters, including money laundering. Without an applicable MLAT (or equivalent lawful mechanism), the compliance officer may be restricted to responding only to domestic authorities, requiring the foreign official to route the request through their own competent authority and the compliance officer's country's competent authority. This is consistent with ACAMS guidance on international cooperation and the use of formal legal channels for cross-border information sharing.

References: UNODC – Mutual Legal Assistance; FATF – Mutual legal assistance

QUESTION NO: 2

According to the Financial Action Task Force, financial institutions should be required to implement:

A. special procedures for encryption of information to be exchanged with affiliates and branches.

B. independent AML programs to ensure privacy and safeguard confidential information.

C. a process to designate an officer at a senior level who ensures a safe exchange of information for AML and terrorism financing purposes.

D. group-wide programs, including policies and procedures regarding AML compliance.

ANSWER: D

Explanation:

"Group-wide programs, including policies and procedures regarding AML compliance." is correct because FATF Recommendation 18 requires financial institutions to have internal controls and procedures to manage ML/TF risk, and—where the institution is part of a financial group—to implement group-wide AML/CFT programmes. These group-wide programmes are intended to ensure consistent standards across the group and typically include group-wide policies and procedures for AML/CFT, compliance management arrangements, information-sharing for AML/CFT purposes within the group, screening procedures to ensure high standards when hiring employees, ongoing training, and an independent audit function to test the programme. The core FATF expectation is not a narrow technical control (like encryption) or a single designated officer focused on "safe exchange," but a comprehensive, risk-based programme applied across the group to support effective prevention, detection, and reporting of suspicious activity and to ensure that branches and majority-owned

subsidiaries apply AML/CFT measures consistent with the home entity's standards (subject to local law constraints). See FATF Recommendation 18 and its interpretive guidance in the FATF Recommendations and the related explanatory/interpretive materials.

References: FATF Recommendations; International Standards (incl. Recommendation 18).

QUESTION NO: 3

Which is the first valid step in the Mutual Legal Assistance Treaties (MLAT) international cooperation process?

A. The central authority that receives the request sends it to a local judicial officer to find out if the information is available.

B. The central authority of the requesting country sends a commission letter of request to the central authority of the other country.

C. The investigator may remove the evidence collected without asking permission to do so.

D. An investigator from the requesting country visits the country where the information is sought and takes statements from the identified witnesses or suspects.

ANSWER: B

Explanation:

The first valid step in the MLAT process is for the requesting state to transmit a formal mutual legal assistance request through its designated central authority to the central authority of the requested state. In practice, MLATs are designed to ensure requests are made government-to-government (not investigator-to-investigator) and follow agreed legal channels, typically requiring a written request (often described as a "letter of request" or "commission rogatoire") that specifies the assistance sought, the legal basis, relevant facts, and any procedural requirements (e.g., confidentiality, form of evidence, deadlines). This central-authority-to-central-authority transmission is the starting point because it triggers the requested state's legal review for treaty/dual criminality/grounds for refusal and enables lawful execution under the requested state's domestic procedures. Only after the request is properly received and accepted can it be routed internally for execution by competent judicial, prosecutorial, or law enforcement bodies. This approach aligns with UNODC guidance on MLA frameworks and the central authority model used internationally for efficient, legally valid cooperation.

References: UNODC Mutual Legal Assistance (MLA) Request Writer Tool / eBook (PDF); UNODC – United Nations Convention against Transnational Organized Crime (MLA framework)

QUESTION NO: 4

When implementing a risk-based approach related to casinos, which risks are related to the customer as an individual? (Choose two.)

A. Transfer between customers

B. Casual customers

C. Improper use of third parties as customers

D. Customer from a high-risk country

E. Use of casino deposit accounts by the customer

ANSWER: C D

Explanation:

In a casino risk-based approach, "customer-as-an-individual" risk factors focus on who the customer is and how they may be using their identity or personal profile to facilitate money laundering. Two classic individual-customer risks are the use of nominees/third parties and the customer's geographic/ML risk profile. "Improper use of third parties as customers" is an individual-level risk because it indicates potential nominee activity (standing in for the true beneficial owner), which is a

common typology to obscure source of funds and ownership/control. “Customer from a high-risk country” is also an individual-level risk factor because the customer’s residence/nationality/links to jurisdictions with higher ML/TF risk directly affects the inherent risk rating and the level of due diligence expected (e.g., enhanced due diligence, source of funds/wealth corroboration). These align with FATF’s risk-based approach concepts and casino sector guidance that emphasize customer risk factors such as geography and use of intermediaries/nominees. See FATF’s RBA guidance and jurisdictional risk concepts: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach.html and FATF high-risk jurisdictions listing context: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html.

QUESTION NO: 5

Which method to finance terrorism involves falsifying transaction-related documents?

A. Bribery

B. Black market peso exchange

C. Trade-based money laundering

D. Informal value transfer system

ANSWER: C

Explanation:

Trade-based money laundering is the method that characteristically involves falsifying transaction-related documents (for example, invoices, bills of lading, customs declarations, and shipping/insurance paperwork) to disguise the true nature, value, quantity, or end-use of goods and services. In the terrorism financing context, these document manipulations can be used to move value across borders under the cover of legitimate trade, generate or shift funds to support terrorist activity, or conceal the parties ultimately benefiting from the transaction. Common TBML techniques include over- and under-invoicing, multiple invoicing, misdescription of goods, and phantom shipments—each relying heavily on altered or fraudulent trade documentation to create a plausible audit trail while obscuring the real flow of value. ACAMS-aligned best practice recognizes TBML as a key typology because it exploits the complexity and volume of global trade, making detection difficult without strong trade documentation review, counterparty due diligence, and anomaly detection across pricing, routing, and shipment data. For further reference, see FATF’s work on trade-based money laundering and terrorism financing risk indicators and typologies: FATF – Trade-based money laundering and FATF – Terrorist financing.

QUESTION NO: 6

How should law enforcement obtain documentation from an institution when suspicious activity was identified? (Choose two.)

A. Request copies of the relevant documents from the accountable institution.

B. Pay an employee of the accountable institution to make copies of the documents.

C. Request a Financial Intelligence Unit (FIU) share copies of suspicious transaction reports.

D. Request the documents from the FIU.

E. Acquire a search warrant to obtain the documents.

ANSWER: A E

Explanation:

When suspicious activity is identified, law enforcement should obtain underlying documentation through formal legal process directed to the financial institution, rather than attempting to obtain or rely on the suspicious activity report itself. In practice, investigators typically request records directly from the institution (for example, account statements, deposit items, wire records, KYC/CDD files, and related internal records) using appropriate compulsory process such as

subpoenas/summonses or other lawful demands, depending on jurisdiction. Where needed—particularly if there is a risk of destruction of evidence or a need for immediate access—law enforcement may also use a search warrant to seize records. This approach aligns with SAR confidentiality rules: SARs (and information that would reveal a SAR was filed) are generally not to be disclosed, and law enforcement should not ask an FIU to “share copies” of SARs as a substitute for obtaining the underlying business records. The key is to obtain admissible, source documentation from the institution via lawful process while maintaining SAR confidentiality.

References: FinCEN SAR Confidentiality (Federal Register); 31 CFR 1020.320 (SAR rule for banks)

QUESTION NO: 7

Which actions are involved when a prosecutor instructs a bank to freeze the assets and bank accounts held by one of its clients? (Choose three.)

A. Inform other banks in the same geographical area to freeze the client's assets if they are a member of that bank, too.

B. Extend the account and asset freeze to the client's family members as a precautionary measure.

C. Ensure the client and beneficiaries are unable to access any frozen assets during the freeze order.

D. The institution does not need to comply with the request if the client's assets make the task unusually difficult or complex to access.

E. An affidavit must accompany the freeze order for the bank to comply with the request.

F. The institution should obtain a copy of the court order to freeze the assets of the named individuals.

G. Implement an immediate hold/block on the specified accounts/assets in accordance with the order’s scope and duration.

ANSWER: C F G

Explanation:

When a prosecutor (typically via a court-authorized restraint/freezing order, seizure warrant, or similar legal process depending on jurisdiction) instructs a bank to freeze a client’s assets, the bank’s core actions are to validate and document the legal authority, implement an immediate hold, and ensure no access or movement of the restrained funds occurs. Operationally, this means the institution should obtain and retain the relevant court order (or other competent legal instrument) identifying the named individual(s) and the scope of property/accounts to be restrained, then apply system blocks so the client and any beneficiaries cannot withdraw, transfer, pledge, or otherwise deal with the frozen assets for the duration of the order. In practice, banks also follow internal escalation and legal review procedures to ensure the freeze is applied correctly and consistently with the order’s terms, and they maintain an audit trail of actions taken. These steps align with CAMS-level best practices around responding to law-enforcement legal process and preserving assets for potential forfeiture/confiscation proceedings. See general guidance on restraint/confiscation measures and international AML frameworks at FATF Recommendations and an overview of asset restraint/forfeiture concepts at UNODC Asset Recovery.

QUESTION NO: 8

A bank employee reviews wire transactions looking for indications of wire stripping.

Which two actions should the employee take to complete appropriate bank procedures? (Choose two.)

A. Compare the wire transaction as it enters and after it leaves the bank

B. Check for suspicious phrases usually used to conceal originator or beneficiary identity

C. Identify large incoming wire transactions received on behalf of a foreign client with no explicit reason

D. Identify wire transaction activity to or from a financial institution located in a higher risk jurisdiction

ANSWER: A B

Explanation:

Wire stripping typically involves removing or altering required payment message information (especially originator/beneficiary details) as a wire moves through one or more intermediary institutions, often to evade sanctions screening, AML monitoring, or transparency requirements. Appropriate bank procedures therefore focus on detecting changes to key data elements across the wire's lifecycle and identifying red flags that suggest intentional obfuscation. Comparing the wire transaction as it enters and after it leaves the bank is a core control because it can reveal whether mandatory fields or identifying information were deleted, truncated, or replaced during processing (including at repair, formatting, or message conversion steps). In addition, checking for suspicious phrases used to conceal originator or beneficiary identity aligns with common typologies where free-text fields, placeholders, or vague descriptors are used to mask parties or reroute screening outcomes. These actions directly target the mechanics of stripping (data alteration and concealment) rather than broader, non-specific risk indicators. For additional context on wire stripping enforcement themes and expectations around transparency in payment messages, see FinCEN advisory on sanctions evasion typologies and red flags and an overview discussion of wire stripping cases at Lexology.

QUESTION NO: 9

What is an example of the integration stage of money laundering involving a bank or another deposittaking institution?

A. Depositing illicit funds into an account set up for a front company
Directing third parties to exchange illicit cash for negotiable instruments

B. Wiring illicit funds from an account at one bank to an account at another bank

C. Using illicit funds that had previously been deposited to purchase a luxury vehicle

ANSWER: C

Explanation:

The integration stage is the point in the money-laundering cycle where the launderer reintroduces the "cleaned" funds into the legitimate economy so they appear to come from lawful sources. In practice, this often looks like using funds that have already been placed into, and moved through, the financial system to buy goods, services, or assets in a way that resembles normal consumer or business activity. "Using illicit funds that had previously been deposited to purchase a luxury vehicle" is a classic integration example because it converts laundered value into an apparently legitimate asset (the vehicle), typically supported by plausible documentation (purchase contract, title/registration, insurance) that can help the criminal explain wealth and spending. ACAMS-style typologies commonly describe integration as purchases of high-value assets (vehicles, real estate, jewelry), investments, or business revenues funded by laundered proceeds after placement and layering have reduced the direct link to the original crime. For additional background on the three stages and integration typologies, see FATF Recommendations (context and typologies) and UNODC Money Laundering Overview.

QUESTION NO: 10

How does the Egmont Group assist financial intelligence unit members to accomplish their goals? (Select Three.)

A. Provides support to expand and systematize cooperation related to the reciprocal exchange of information

B. Fosters better and secure communication through the application of technology

C. Develops official lists of suspected terrorists on a globally coordinated basis by relevant authorities

D. Encourages operational autonomy of financial intelligence units

E. Maintains uniform global formats for funds transfers that assist in the detection of money laundering

F. Supplies information on the common money laundering tactics used by terrorists and financial supporters of terrorism

ANSWER: A B D

Explanation:

The Egmont Group is a global network of Financial Intelligence Units (FIUs) created to strengthen FIUs' ability to fight money laundering, associated predicate offenses, and terrorist financing through practical international cooperation. In line with its published mission and objectives, it helps FIU members by supporting and systematizing cooperation for the reciprocal exchange of financial intelligence (including facilitating information sharing between FIUs), and by fostering secure communication through technology—most notably via the Egmont Secure Web (ESW), which enables trusted, encrypted FIU-to-FIU exchanges. The Egmont Group also promotes FIU effectiveness and independence by encouraging operational autonomy and providing a forum for best practices, training, and typologies work that supports FIUs' analytical and operational capabilities. These functions are core to how Egmont enables FIUs to accomplish their goals: improving the speed, security, and consistency of cross-border intelligence sharing while strengthening FIU capacity and governance. See the Egmont Group overview and mission statements for the FIU cooperation and secure information-sharing focus: https://egmontgroup.org/ and the description of FIUs and their role in information exchange: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

QUESTION NO: 11

Which three entities does the Third European Union Money Laundering Directive apply to?

A. Financial Institutions

B. Defense Attorneys

C. Casinos

D. Real Estate Agents

ANSWER: A C D

Explanation:

The Third EU Money Laundering Directive (Directive 2005/60/EC) applies to a broad set of "obliged entities," including core financial sector firms and a range of designated non-financial businesses and professions. Financial institutions are covered because the directive is designed to prevent misuse of the financial system and therefore imposes customer due diligence, recordkeeping, and suspicious transaction reporting obligations on banks and other financial sector firms. Casinos are explicitly included as obliged entities due to their higher inherent ML/TF risk and the ease with which cash can be introduced and layered through gaming activity. Real estate agents are also covered because property transactions can be used to launder large sums and obscure beneficial ownership, so the directive extends AML obligations to intermediaries involved in buying and selling real property. These categories align with ACAMS best-practice understanding of EU AML frameworks: the directive targets both the financial system and key "gatekeeper" sectors where criminals commonly place or integrate illicit funds. For the primary legal text and scope, see EUR-Lex: Directive 2005/60/EC. For additional EU AML context and obliged-entity coverage, see European Commission AML/CFT overview.

QUESTION NO: 12

Under the Wolfsberg Correspondent Banking Principles, which action is considered an enhanced due diligence obligation to correspondent banking clients that present greater risks?

A. Conducting reviews on all high-risk relationships

B. An evaluation done by the compliance officer in charge of the account

C. Approval of a high-risk relationship by a senior management committee

D. Ongoing monitoring of clients located in tax haven countries

ANSWER: C

Explanation:

Under the Wolfsberg Correspondent Banking Principles, enhanced due diligence for higher-risk correspondent banking relationships includes applying stronger governance and escalation, particularly ensuring that the decision to onboard or continue a higher-risk relationship is reviewed and approved at an appropriately senior level. The principles emphasize that higher-risk correspondents should be subject to enhanced scrutiny and controls commensurate with the risk, and that this typically involves escalation to senior management (or an appropriate committee) for approval, along with documented rationale and oversight. This senior-level approval is a hallmark of enhanced due diligence because it demonstrates that the institution has recognized the elevated risk, applied additional checks, and accepted the risk knowingly within its risk appetite and control framework. This approach aligns with broader AML best practice and regulatory expectations that higher-risk relationships receive enhanced governance, including senior management involvement, as part of a risk-based program. See the Wolfsberg Group's correspondent banking guidance and the FATF risk-based approach expectations for higher-risk relationships and enhanced measures.

References: Wolfsberg Group – Principles and Guidance; FATF Recommendations (risk-based approach and enhanced measures)

QUESTION NO: 13

An institution has made the decision to exit a client relationship due to anti-money laundering concerns. Prior to starting the close out process, the institution receives a written request from a law enforcement agency to keep the account open. The client is the subject of an ongoing investigation and law enforcement wants the institution to continue to monitor the account and report any suspicious activity.

What is a primary consideration the institution should keep in mind when deciding whether to agree to this request?

A. The anticipated cost of complying with the law enforcement request

B. The number of suspicious transaction reports previously filed on the client

C. The fact that the institution has a solid record in complying with law enforcement requests

D. Whether the institution can continue to meet its regulatory obligations with the accounts open

ANSWER: D

Explanation:

The key consideration is whether keeping the account open allows the institution to continue meeting all applicable legal and regulatory obligations while managing the risk. Even when law enforcement requests that an account remain open to support an investigation, the institution does not outsource its AML responsibilities: it must still apply its risk-based controls, conduct ongoing monitoring, file SARs/STRs when warranted, and ensure it can manage exposure to money laundering, sanctions, fraud, and reputational risk. In practice, this means confirming the request is properly documented, assessing whether enhanced monitoring and controls are feasible, and ensuring the relationship can be maintained without violating internal policies, risk appetite, or regulatory expectations (for example, if the activity is so severe that the institution cannot reasonably mitigate the risk). If the institution cannot maintain compliance—e.g., it cannot adequately monitor, cannot manage the risk, or would breach policy/regulatory expectations—then keeping the account open would be inappropriate even with a request. This aligns with the broader CAMS/AML principle that decisions to maintain or exit relationships must be grounded in the institution's ability to control risk and comply with obligations, not primarily on cost, past SAR counts, or general cooperation history. See FinCEN Guidance and FFIEC BSA/AML Examination Manual (Ongoing Monitoring overview).

QUESTION NO: 14

Which elements can trigger a review of the existing relationship during the opening of a new account? (Select Two.)

A. Regular checks on the flow of funds

B. Recent adverse media on the client

C. A false positive result for name screening

D. Incoming transfers from high-risk jurisdictions

E. Estimated total income decrease

ANSWER: B D

Explanation:

During new account opening, institutions commonly reassess the broader customer relationship when new information suggests elevated ML/TF risk or a material change in the customer's risk profile. Two well-established triggers are recent adverse media on the client and incoming transfers from high-risk jurisdictions. Adverse media can indicate potential involvement in fraud, corruption, sanctions evasion, or other predicate offenses, and it often requires enhanced due diligence, refreshed KYC, and potentially escalation depending on severity and credibility. Similarly, activity connected to high-risk jurisdictions (including jurisdictions with strategic AML/CFT deficiencies, high corruption, or significant sanctions exposure) is a classic risk indicator that can warrant reviewing the customer's expected activity, source of funds/wealth, beneficial ownership, and the adequacy of existing controls. These triggers align with risk-based customer due diligence and ongoing monitoring expectations described in FATF guidance and widely reflected in CAMS best practices for periodic and event-driven reviews. See FATF's guidance on the risk-based approach and ongoing CDD (https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach.html) and FATF Recommendation 10 on customer due diligence (https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html).

QUESTION NO: 15

Which risks are involved in a correspondent banking client's ownership and management structure? (Select Two.)

A. Regularity of board meetings

B. Size of the management structure

C. Status as a state, publicly, or privately held entity

D. Length of time since the last Wolfsberg Group review

E. Transparency of the ownership structure

ANSWER: C E

Explanation:

For correspondent banking, ACAMS-aligned due diligence focuses heavily on understanding who owns and controls the respondent institution and whether that structure creates opacity or undue influence. Two core risk considerations tied directly to ownership and management structure are the client's status as a state-owned, publicly listed, or privately held entity and the transparency of the ownership structure. Entity status matters because state ownership can introduce political exposure and governance concerns, while privately held entities can present higher opacity risk if ownership is concentrated or not well documented. Transparency of ownership is central to identifying beneficial owners, controllers, and potential use of nominees, shell entities, or complex layering that can conceal sanctioned parties, PEPs, or criminal proceeds. These factors are consistently emphasized in correspondent banking guidance as key inputs to risk rating and to determining the depth of enhanced due diligence, including verifying beneficial ownership and understanding governance/control. See the FATF guidance on correspondent banking and transparency expectations and the Wolfsberg Correspondent Banking Due Diligence Questionnaire materials commonly used to assess ownership/control information: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-correspondent-banking.html and https://www.wolfsberg-principles.com/.

QUESTION NO: 16

After a FATF mutual evaluation process, which are resulting actions for jurisdictions that are determined to have strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing? (Choose two.)

A. Expect private statements from FATF regarding the level of compliance of the jurisdiction, when insufficient progress is made.

B. Appeal to FATF for a technical compliance re-rating based on the jurisdiction's own experts criteria.

C. Demonstrate a high-level commitment to swiftly resolve the identified deficiencies in the FATF mutual evaluation report.

D. Request FATF for an extension of deadlines in order to provide local awareness on the improvements that are necessary to solve the deficiencies.

E. Report to FATF on the implementation of their progress under the enhanced follow-up mechanism.

ANSWER: C E

Explanation:

When a jurisdiction is found to have strategic AML/CFT/CPF deficiencies following the FATF mutual evaluation and is placed under FATF's monitoring processes, FATF expects concrete, ongoing remediation and accountability at the highest levels. A key resulting action is that the jurisdiction must demonstrate a high-level political commitment to address the deficiencies identified in the mutual evaluation, typically by agreeing to an action plan and prioritizing rapid implementation of reforms. In addition, FATF requires the jurisdiction to report back on progress in implementing the agreed measures under the relevant follow-up/monitoring process (often described as enhanced follow-up or increased monitoring), so FATF can assess whether the jurisdiction is making sufficient progress and whether further FATF steps are warranted. These actions align with FATF's public statements on "high-risk and other monitored jurisdictions," which describe jurisdictions' commitments and the expectation of regular progress reporting against action plans. See FATF's overview of monitored jurisdictions and the increased monitoring process: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions.html and FATF's explanation of mutual evaluations and follow-up: https://www.fatf-gafi.org/en/topics/mutual-evaluations.html.

QUESTION NO: 17

The local manager of a remote mortgage origination department of a financial institution has just discovered that sanctions screening of new customers is not being performed.

Which action should the local manager take in this situation?

A. Start screening new customers

B. Immediately inform the regulators

C. Immediately inform senior management

D. Do nothing because the department only handles a very small number of mortgages

ANSWER: C

Explanation:

Immediately inform senior management is the appropriate action because a failure to perform sanctions screening is a significant compliance control breakdown that creates immediate legal, regulatory, and reputational exposure for the institution. Under an effective AML/sanctions compliance program, issues of this severity must be escalated promptly through established governance channels so the institution can (1) stop or contain the risk, (2) implement corrective actions (e.g., immediate screening, backlog remediation, and potential account/transaction holds), (3) assess whether any prohibited parties were onboarded, and (4) determine whether notifications to regulators or other authorities are required based on applicable rules and internal policy. Senior management oversight is a core expectation in AML/sanctions programs, including ensuring adequate resources, controls, and timely remediation of deficiencies. Escalation also supports proper documentation, independent review, and coordination with compliance/legal to manage potential reporting obligations and to prevent inconsistent or unauthorized external communications. This aligns with widely accepted compliance program principles emphasizing management accountability and prompt escalation of material control failures. See OFAC's compliance framework for expectations around management commitment and escalation/remediation: https://ofac.treasury.gov/ofac-compliance-framework and the FFIEC BSA/AML guidance on compliance program governance and oversight: https://bsaaml.ffiec.gov/manual.

QUESTION NO: 18

Which information should be gathered as part of enhanced due diligence (EDD) for a high-risk customer?

A. Explanation's for changes in marital status

B. Details on individuals with control over the account

C. Plans for traveling in business trips

D. Personal references

ANSWER: B

Explanation:

Details on individuals with control over the account is a core element of enhanced due diligence for higher-risk relationships because EDD is designed to deepen the institution's understanding of who ultimately owns, controls, and can direct activity in the relationship. For high-risk customers, it is not sufficient to identify only the named account holder; the institution should also identify and verify relevant beneficial owners, authorized signers, directors/partners, trustees/protectors (as applicable), and any other persons who can exercise control or influence over the account or customer entity. This information supports a more accurate risk assessment, helps establish expected account activity, and strengthens ongoing monitoring by enabling the institution to detect unusual behavior tied to specific controllers (e.g., sudden changes in signatories, use of intermediaries, or activity inconsistent with the controller's profile). ACAMS-aligned best practice and regulatory expectations emphasize understanding ownership/control and the purpose and intended nature of the relationship as key EDD outcomes for higher-risk customers. See FATF guidance on customer due diligence and beneficial ownership: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html and the Wolfsberg Group CDD guidance: https://www.wolfsberg-principles.com/.

QUESTION NO: 19

A compliance officer at a financial institution (FI) received an investigation request for a customer from a local law enforcement agency. Which action should be taken by the FI?

A. Obtain approval from the Financial Intelligence Unit (FIU) before submitting the customer's information.

B. Omit some responses to meet the regulatory deadline.

C. Assign employees responsible for the customer to the investigation team.

D. Consider retaining qualified, experienced legal counsel.

ANSWER: D

Explanation:

Consider retaining qualified, experienced legal counsel. When a financial institution receives an investigation request from local law enforcement, the institution must ensure the request is valid, properly authorized, and handled in a way that complies with applicable privacy, bank secrecy, and data-protection obligations. Legal counsel can quickly assess whether the request is a subpoena, court order, summons, or informal request; determine what information can be disclosed; confirm any required customer-notification restrictions; and guide the institution on preserving records and maintaining appropriate confidentiality. This is consistent with AML best practice: law enforcement inquiries can create legal and regulatory exposure if the institution discloses too much, too little, or to the wrong party, or if it mishandles privileged or protected information. Counsel also helps coordinate internal stakeholders (compliance, investigations, operations, and information security) and ensures responses are accurate, complete, and defensible, including documenting the basis for disclosure. In many jurisdictions, there is no general requirement to obtain FIU approval before responding to law enforcement; instead, institutions respond based on the legal authority of the request and applicable laws and policies. See guidance on responding to law enforcement legal process and protecting customer information: FFIEC BSA/AML Manual – Office of Law Enforcement Liaison and FinCEN Guidance.

QUESTION NO: 20

Which three measures are contained in Financial Action Task Force 40 Recommendations for reporting suspicious activity? (Choose three.)

A. The activity should be reported promptly to the country's financial intelligence unit.

B. The financial institution has been contracted by law enforcement regarding the activity.

C. The financial institution has grounds to believe the activity is related to terrorist financing.

D. The financial institution has contacted the account holder to determine the activity of the account.

E. The financial institution has reasonable grounds to suspect the funds are proceeds of criminal activity.

ANSWER: A C E

Explanation:

FATF Recommendation 20 sets out the core requirements for suspicious transaction/activity reporting. It requires that when a financial institution suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity, it must report that suspicion. The same obligation applies when the suspicion relates to terrorist financing, reflecting the FATF's expectation that STR/SAR regimes cover both money laundering predicate offenses and terrorist financing risks. In addition, the recommendation specifies that such reports must be made promptly to the country's financial intelligence unit (FIU), which is the designated national center for receiving and analyzing STRs/SARs and disseminating intelligence to competent authorities. These elements together capture the "trigger" for reporting (suspicion or reasonable grounds), the scope of suspicion (criminal proceeds and terrorist financing), and the destination/timeliness of reporting (promptly to the FIU). They are foundational measures in the FATF 40 Recommendations and are widely implemented in national AML/CFT laws and regulatory expectations.

References: FATF Recommendations (incl. Recommendation 20); FATF 40 Recommendations overview.

QUESTION NO: 21

A retail bank prepares a yearly AML risk assessment. Which inherent risk factor is likely the most relevant?

A. The provision of remote check deposit services

B. The provision of cash services

C. The provision of payable through accounts

D. The provision of brokerage services

ANSWER: B

Explanation:

The provision of cash services is typically the most relevant inherent AML risk factor for a retail bank because cash is highly anonymous, easily transferable, and difficult to trace compared with most non-cash payment methods. Retail banking channels (branches, ATMs, cash deposits/withdrawals, cash-intensive customer segments) create frequent opportunities for placement of illicit proceeds into the financial system, including structuring/smurfing, rapid cash-in/cash-out activity, and the use of third parties or false identities to obscure beneficial ownership. In an inherent risk assessment, this factor is evaluated before considering mitigating controls (e.g., transaction monitoring, CTR/threshold reporting, customer due diligence, and branch controls). ACAMS-aligned risk frameworks commonly treat products and services that enable cash movement as higher inherent risk due to the elevated likelihood and impact of money laundering typologies involving physical currency. This is why, for a retail bank's annual AML risk assessment, cash services are usually a primary driver of inherent risk ratings across products, customers, geographies, and delivery channels.

References: FFIEC BSA/AML Examination Manual; FATF Recommendations.

QUESTION NO: 22

A local law enforcement officer, who is conducting a criminal investigation, requests information about a customer.

Which two actions should the bank take? (Choose two.)

A. Close the account immediately

B. File a suspicious transaction report

C. Monitor the account for suspicious activity

D. Review the money laundering risk posed by the account

ANSWER: B C D

Explanation:

When law enforcement requests customer information in connection with a criminal investigation, the bank should treat the request as a potential risk indicator and respond through appropriate internal and legal channels. A prudent AML response includes enhancing ongoing due diligence by monitoring the account for suspicious activity, looking for unusual patterns, changes in transaction behavior, or activity inconsistent with the customer's profile. In parallel, the bank should reassess the money laundering risk posed by the account—updating the customer risk rating if needed, checking for adverse information, and ensuring controls (such as alert thresholds and review frequency) are appropriate for the updated risk level. These steps align with core CAMS/AML best practices: risk-based customer due diligence and ongoing monitoring as circumstances change. The request itself does not automatically require account closure, and filing a suspicious transaction report is typically driven by the bank's own detection of suspicious activity (or reasonable grounds for suspicion), not merely by an informal inquiry. If the request is accompanied by proper legal process (e.g., subpoena/court order) the bank should follow its established procedures for disclosure while maintaining confidentiality requirements. See FinCEN's overview of SAR expectations and confidentiality (https://www.fincen.gov/resources/statutes-regulations/guidance/suspicious-activity-reporting) and FFIEC BSA/AML guidance on ongoing monitoring and risk-based CDD (https://bsaaml.ffiec.gov/manual).

QUESTION NO: 23

What is an example of a legal risk a financial institution (FI) could face if it is sanctioned for failure to report suspected fraud activity?

A. Foreign correspondents could terminate their relationships with the sanctioned bank.

B. Clients of the bank might draw down the reserves of the bank and lead to liquidity issues.

C. The bank could be forced to reimburse the victims of the fraudster for the losses suffered.

D. The bank could see higher default rates on loans granted to companies owned by the fraudster.

ANSWER: C

Explanation:

A clear example of legal risk from being sanctioned for failing to report suspected fraud is being exposed to civil liability—such as lawsuits or regulatory/consumer redress actions—where the institution may be required to compensate harmed parties. If an FI fails to file required reports (for example, suspicious activity reports) or otherwise fails to meet statutory reporting obligations, regulators can impose penalties and, depending on the jurisdiction and facts, the FI can also face private litigation alleging negligence, breach of duty, or facilitation of fraud. Those legal actions can result in court-ordered damages, settlements, restitution, or mandated remediation programs. This is distinct from reputational or liquidity impacts; it is specifically about legal exposure and enforceable obligations arising from laws, regulations, and court processes. In AML best practice terms, this aligns with the concept that noncompliance can trigger enforcement actions and create downstream civil claims when victims argue that earlier detection/reporting could have prevented or reduced losses. For background on SAR obligations and the consequences of noncompliance, see FinCEN's SAR overview (https://www.fincen.gov/resources/statutes-regulations/guidance/suspicious-activity-reporting) and the FFIEC BSA/AML Examination Manual discussion of SARs and enforcement expectations (https://bsaaml.ffiec.gov/manual).

QUESTION NO: 24

Which statement best describes a key aspect of the AML Directive of the EU regarding business relationships and transactions with high-risk third countries?

A. Obliged entities should voluntarily consider the implementation of increased external audit requirements for branches and subsidiaries located in high-risk countries.

B. Obliged entities, in accordance with the member state regulations, should determine at a national level the measures that can be used for enhanced due diligence.

C. Obliged entities should implement additional mitigating measures complementary to the enhanced customer due diligence procedures, in accordance with a risk based approach.

D. Obliged entities should not take into account specific circumstances when performing enhanced due diligence measures.

ANSWER: C

Explanation:

Under the EU AML framework (notably the 4th AMLD as amended by the 5th AMLD), when dealing with business relationships or transactions involving high-risk third countries identified by the EU, obliged entities must apply enhanced due diligence (EDD). A key aspect is that EDD is not a “check-the-box” exercise: firms are expected to apply a risk-based approach and, where appropriate, add mitigating controls that go beyond baseline EDD steps. This is reflected in the directive’s expectation that institutions implement additional measures to manage and mitigate the heightened ML/TF risks posed by such jurisdictions (for example, obtaining additional information on the customer and beneficial owner, understanding source of funds/wealth more deeply, increasing monitoring intensity/frequency, and applying senior management approval). The statement that obliged entities should implement additional mitigating measures complementary to enhanced customer due diligence procedures, in accordance with a risk based approach, best captures this core requirement and the practical compliance expectation across EU member states.

References: Directive (EU) 2015/849 (4th AMLD) – EUR-Lex; European Banking Authority AML/CFT resources.

QUESTION NO: 25

Based on studies executed by the Organization for Economic Cooperation and Development (OECD), which occupations are particularly vulnerable to the use of false identities and identity theft?

A. Government officers

B. Sea port officers

C. Lawyers

D. Laborers

ANSWER: C

Explanation:

The correct answer is “Lawyers” because OECD work on identity fraud and misuse of professional “gatekeepers” highlights that certain professions are especially exposed to criminals using false identities to access services, move funds, or create legal structures that obscure beneficial ownership. Lawyers (along with other professional service providers such as accountants and trust/company service providers) can be targeted because they may open client accounts, handle escrow/settlement funds, establish companies or trusts, and act as intermediaries in high-value transactions. These activities create opportunities for criminals to present forged or stolen identity documents, impersonate legitimate clients, or use nominees, particularly where customer due diligence is weak or where professional secrecy is misused. From an AML perspective, this aligns with ACAMS guidance that “gatekeepers” are higher-risk touchpoints requiring robust client identification/verification, beneficial ownership checks, and ongoing monitoring to mitigate impersonation and identity theft risks. In short, the combination of access to the financial/legal system, ability to create or manage legal

persons/arrangements, and the perceived legitimacy conferred by professional involvement makes lawyers particularly vulnerable to identity fraud schemes.

References: OECD – Anti-corruption and integrity (resources on identity fraud and misuse of intermediaries); FATF – Risk-Based Approach for Legal Professionals

QUESTION NO: 26

A company service provider in Country A sets up a corporate structure for a client from Country B, which is known for corruption. The corporate structure includes a holding company in Country A with a bank account in one of the international banks located there.

During on-boarding, the client's wealth was estimated at $7 million. Shortly thereafter, the client's father became president of Country

B. During a routine client review two years later, it was identified that client's wealth had grown to $510 million.

What are two red flags that indicate money laundering or financial terrorism? (Choose two.)

A. The client is from a country known for corruption.

B. During a routine client review two years later, it was identified that client's wealth had grown to $510 million.
What are two red flags that indicate money laundering or financial terrorism? (Choose two.)

The substantial growth in wealth during a short period of time.

C. The client is a family member of a PEP from a country known for corruption.

D. The holding company is in Country A with a bank account in one of the international banks.

ANSWER: B C

Explanation:

The key red flags are the client's close association with a politically exposed person and the sudden, unexplained increase in wealth. When a client's father becomes president, the client is considered a family member of a PEP, which materially elevates ML/FT risk because of the potential for bribery, embezzlement, and abuse of public office; this is especially acute when the relevant jurisdiction is known for corruption. In addition, a jump in estimated wealth from $7 million to $510 million over roughly two years is a classic "source of wealth/source of funds" concern and should trigger enhanced due diligence, refreshed beneficial ownership and control checks, and deeper corroboration of how the wealth was generated (e.g., legitimate business sale, inheritance, public disclosures) along with more intensive monitoring. ACAMS-aligned best practice is to treat PEP relationships and unexplained wealth accumulation as heightened-risk indicators requiring stronger controls rather than relying on the mere existence of a holding company or an international bank account as a standalone red flag. See FATF guidance on PEP risk management and EDD expectations: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Politically-exposed-persons.html and FATF Recommendations (customer due diligence/EDD): https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

QUESTION NO: 27

A Money Laundering Reporting Officer's (MLRO) lack of action led to deficiencies in the bank's AML program and a civil monetary penalty being levied against the MLRO. Why was this direct action taken against the MLRO?

A. The MLRO is the only individual that can be held responsible for AML program deficiencies.

B. MLROs can be held to an individual accountability standard and face potential penalties for contributing to AML program deficiencies.

C. The MLRO agreed to the civil penalty so that the bank would not be found liable for the AML program deficiencies.

D. Action was brought against the MLRO because banks cannot be found liable for AML program deficiencies.

ANSWER: B

Explanation:

Direct action can be taken against an MLRO because, in many jurisdictions and regulatory frameworks, the MLRO (or equivalent AML compliance officer) is a designated "responsible person" with specific, personal duties to oversee the effectiveness of the AML program and to ensure appropriate escalation and reporting of suspicious activity. Where an MLRO's omissions or failures materially contribute to program breakdowns—such as not implementing required controls, not remediating known gaps, or not ensuring timely suspicious activity reporting—regulators may pursue individual accountability in addition to, or alongside, action against the institution. This reflects the broader supervisory trend toward holding senior managers and control function leaders personally accountable when their conduct falls below expected standards and results in AML control failures. In practice, this means an MLRO can face civil monetary penalties, prohibition orders, or other sanctions when their own actions (or inaction) are deemed to have contributed to AML deficiencies, even though the bank itself can also be held liable. This individual-accountability concept is consistent with how regulators describe compliance officer responsibilities and enforcement approaches in AML matters.

References: FinCEN Guidance; UK FCA – Senior Managers & Certification Regime (SM&CR)

QUESTION NO: 28

What is an aspect of the USA PATRIOT Act that has extraterritorial reach?

A. To strengthen US measures to prevent, detect and prosecute international money laundering and financing of terrorism.

B. To implement economic and trade sanctions based on US foreign policy.

C. To mandate stricter money laundering controls across the continent.

D. To require scrutiny of foreign financial institutions (FIs) and classes of international transactions that are susceptible to criminal abuse.

ANSWER: D

Explanation:

The USA PATRIOT Act has extraterritorial reach where it targets risks and conduct outside the United States that can affect the U.S. financial system. A key example is the Act's focus on foreign financial institutions and cross-border activity—particularly provisions in Title III (International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001) that require enhanced scrutiny of certain foreign banks, correspondent banking relationships, and categories of international transactions that are vulnerable to abuse. In practice, these provisions can obligate U.S. financial institutions to apply due diligence and enhanced due diligence measures to foreign correspondent accounts and private banking accounts, and they also empower U.S. authorities to take actions that impact foreign institutions (for example, through special measures or restrictions when a foreign jurisdiction, institution, or transaction class is deemed of primary money laundering concern). This is "extraterritorial" in effect because it compels risk controls and scrutiny that reach beyond domestic customers and domestic activity, extending to foreign counterparties and international flows that interface with the U.S. financial system.

References: FinCEN – USA PATRIOT Act; Public Law 107-56 (USA PATRIOT Act text).

QUESTION NO: 29

What are the European Union Directives on Money Laundering?

A. They are voluntary codes of best practice for the financial sector

B. They are written by the Wolfsberg Group

C. They require members to implement certain laws of prevent money laundering

D. They require financial institutions to report suspicious activity to the Egmont Group in Brussels

ANSWER: C

Explanation:

European Union anti-money laundering directives are binding legislative instruments that set out minimum standards each EU Member State must achieve by transposing the directive's requirements into national law. In CAMS terms, this is a core feature of EU directives: they do not operate as optional guidance, but instead obligate Member States to implement specific AML/CFT measures—such as customer due diligence, recordkeeping, suspicious transaction reporting frameworks, and supervisory expectations—through domestic legislation and regulation. Historically, this began with the First AML Directive (Directive 91/308/EEC), which required Member States to enact laws to prevent misuse of the financial system for money laundering, and subsequent directives expanded scope and strengthened controls. The key point is that the directives create legal obligations at the Member State level (with practical impact on obligated entities via national implementing rules), rather than being industry-authored best practices or reporting lines to non-EU bodies. See the EU's overview of AML/CFT policy and legislation at European Commission – AML/CFT policy and the text/history of the First AML Directive at EUR-Lex (91/308/EEC).

QUESTION NO: 30

Why do organized crime groups often use front companies? (Choose two).

A. Because they are not registered, front companies are not subject to income and other sales taxes.

B. Because using multiple front companies can make it easier to control an entire sector of the economy.

C. Because they are generally subject to lighter due diligence requirements by banks and other financial services providers.

D. Because front companies generally charge higher prices than legitimate companies, so profit margins are higher.

E. Because they can use the company's bank accounts to comingle deposits with those of legal businesses.

ANSWER: B E

Explanation:

Organized crime groups use front companies primarily to disguise the origin and nature of illicit funds by embedding them in apparently legitimate commercial activity. A front company can generate invoices, contracts, and "business rationale" that make suspicious cash flows look like normal revenue, which helps criminals place and layer proceeds through the financial system with reduced scrutiny. A key benefit is the ability to use the company's bank accounts to commingle criminal proceeds with legitimate business receipts, making it harder for investigators and financial institutions to distinguish illicit deposits from lawful turnover and to trace funds back to predicate offenses.

Front companies also support broader criminal objectives such as gaining influence or control in a market by operating multiple related entities (e.g., suppliers, distributors, service firms). This can enable price manipulation, bid-rigging, or intimidation-backed market capture while maintaining a veneer of legitimacy. These uses align with core AML typologies described in FATF guidance on the misuse of legal persons and in general AML best practices around identifying beneficial ownership, unusual business activity, and inconsistent transaction patterns.

References: FATF/Egmont – Concealment of Beneficial Ownership, FATF Recommendations.

QUESTION NO: 31

A bank teller receives a written request from a police officer to review a previous customer's account on a pre-populated form with the officer's official letter head. The officer suspects the previous customer is engaging in smurfing. Which action should the bank teller perform?

A. Provide the police officer information after AML compliance approval.

B. Reject the request and escalate to the compliance officer.

C. Provide the police officer information after management approval.

D. Escalate the request to the compliance officer.

ANSWER: D

Explanation:

Escalate the request to the compliance officer. A teller should not disclose customer account information based solely on an informal written request, even if it appears official (e.g., letterhead or a pre-populated form). In AML programs, frontline staff are expected to follow established information-sharing and law-enforcement request procedures, which typically require validation of legal authority (such as a subpoena, court order, or other applicable compulsory process) and internal review by the bank's designated function (often Compliance/Legal). Escalation ensures the request is authenticated, properly logged, and handled in line with privacy/bank-secrecy obligations and the institution's policies, while also enabling the bank to consider whether the underlying activity warrants internal investigation and potential suspicious activity reporting. This approach aligns with CAMS best practices: employees identify and refer potential suspicious activity and external requests to the appropriate AML/compliance channel rather than making disclosure decisions themselves. See FinCEN's SAR guidance and confidentiality expectations: https://www.fincen.gov/resources/statutes-regulations/guidance/advisory-suspicious-activity-reporting and general U.S. law-enforcement access mechanisms described by the DOJ: https://www.justice.gov/usao/page/file/988501/dl.

QUESTION NO: 32

How should law enforcement obtain documentation from an institution when suspicious activity was identified? (Choose two.)

A. Request copies of the relevant documents from the accountable institution.

B. Pay an employee of the accountable institution to make copies of the documents.

C. Request a Financial Intelligence Unit (FIU) share copies of suspicious transaction reports.

D. Request the documents from the FIU.

E. Acquire a search warrant to obtain the documents.

ANSWER: A E

Explanation:

When suspicious activity is identified, law enforcement should obtain underlying documentation through proper legal process directed to the financial institution, rather than attempting to obtain or rely on the suspicious transaction report itself. Best practice (and, in the U.S., a legal requirement) is that suspicious activity reports are confidential and generally cannot be disclosed by the filing institution; law enforcement typically should not request the SAR from the institution. Instead, investigators should request the underlying business records (e.g., account opening documents, statements, wire records, KYC/CDD files) directly from the institution via appropriate compulsory process such as a subpoena, summons, or court order, and in some circumstances a search warrant. A search warrant is also a recognized method to obtain documents when probable cause exists and immediate seizure is needed. These approaches align with SAR confidentiality rules and ensure evidence is collected in an admissible, auditable manner. In the U.S., FinCEN's SAR confidentiality guidance emphasizes that SARs are protected and that law enforcement should seek supporting documentation from the institution through proper channels. See FinCEN SAR Confidentiality (Federal Register) and FinCEN Guidance.

QUESTION NO: 33

When should a financial institution (FI) exit a relationship? (Choose two.)

A. The reputational risk to the FI posed by closing the account

B. The request from law enforcement to close the account

C. The FI's requirements for opening an account

D. The suspicious conduct of the account holder

E. The FI's stated policies and procedures for closing an account

ANSWER: C D E

Explanation:

A financial institution should exit a customer relationship when it cannot appropriately manage the money-laundering/terrorist-financing risk within its risk appetite and control framework, or when it cannot meet its legal and internal governance obligations for customer due diligence. In practice, this commonly occurs when the institution's account-opening and ongoing due diligence requirements cannot be satisfied (for example, inability to verify identity/beneficial ownership, obtain required information, or resolve material discrepancies), because the FI cannot maintain a compliant customer risk profile. Exiting is also appropriate when the institution's own documented policies and procedures call for closure based on defined triggers (such as repeated failure to provide required documentation, unacceptable residual risk after enhanced due diligence, or governance decisions tied to risk appetite). These decisions should be executed consistently, documented, and aligned to the FI's customer acceptance/retention standards and account closure processes, including appropriate escalation and legal review where needed. This approach aligns with U.S. banking regulators' expectations that banks maintain effective BSA/AML compliance programs and manage customer relationships consistent with risk-based policies and procedures. See the FDIC's BSA/AML examination resources and FFIEC BSA/AML guidance for risk-based customer management expectations: FDIC BSA/AML Examination Manual and FFIEC BSA/AML Examination Manual.

QUESTION NO: 34

A banker in the credit department wants to assess the risk of all customers, and contacts the compliance officer to request a list of customers with suspicious transaction report filings.

What should be done to protect suspicious transaction report information?

A. Provide the suspicious transaction report information to the credit department

B. Decline to provide the suspicious transaction report information to the credit department

C. Seek approval from the board of directors to disclose the suspicious transaction report information

D. Contact the credit department manager to determine how the suspicious transaction report information can be provided

ANSWER: B

Explanation:

Suspicious transaction report (STR/SAR) information is subject to strict confidentiality and "tipping-off" prohibitions in most AML regimes. A key control is limiting access to STR/SAR existence and content to staff who have a defined need-to-know for AML compliance purposes (e.g., AML investigations, MLRO/Compliance, certain audit functions under controlled conditions). Providing a list of customers with STR filings to a business unit like credit for general risk assessment would typically exceed that need-to-know and could create tipping-off risk, undermine ongoing or future investigations, and breach legal/regulatory confidentiality requirements. Therefore, the appropriate action to protect STR/SAR information is to decline to provide the suspicious transaction report information to the credit department and instead support credit risk objectives through non-STR-derived risk indicators (e.g., customer risk ratings, adverse media, transactional behavior analytics) that do not disclose STR/SAR filing status. This approach aligns with ACAMS best practices around SAR/STR confidentiality and internal controls, ensuring STR/SAR data is compartmentalized and only shared under tightly governed, legally permitted circumstances.

References: FinCEN – Suspicious Activity Reporting; FATF Recommendations (see tipping-off/confidentiality principles).

QUESTION NO: 35

A bank located in Arizona is considering a loan application for a new client. The collateral for the loan is a property in Florida.

The loan will be in the name of a limited liability company (LLC) whose ownership is not disclosed to the bank. The LLC was established by a New York-based attorney.

The loan will be repaid by the LLC in monthly wire transfers of $9,000 which is more than the required monthly payment.

Which aspect indicates the potential for money laundering?

A. The LLC's ownership is not disclosed to the bank

B. The collateral, a property in Florida, is not located in Arizona

C. The repayment in the amount of $9,000 indicates potential structuring

D. The attorney associated with the account is outside the bank's lending area

ANSWER: A C D

Explanation:

The key money-laundering indicators here are the use of an entity that obscures beneficial ownership and the use of payment behavior that can be consistent with layering/placement tactics. When an LLC's ownership is not disclosed to the bank, it raises a significant transparency risk because criminals commonly use legal entities to conceal the true beneficial owner and source of funds. Sound AML practice (and U.S. CDD expectations) requires financial institutions to identify and verify beneficial owners of legal entity customers and to understand the nature and purpose of the relationship; lack of ownership transparency is therefore a classic red flag.

In addition, repeated payments in amounts just under common reporting/monitoring thresholds can be a red flag for structuring-like behavior, even when the instrument is a wire transfer rather than cash. While "structuring" is a term most precisely associated with evading Currency Transaction Reports for cash, AML programs also treat patterns of transactions designed to avoid detection (including threshold-avoidance patterns) as suspicious and potentially indicative of money laundering. These factors together warrant enhanced due diligence and potentially a SAR filing depending on the bank's investigation results.

References: FinCEN CDD Final Rule; FFIEC BSA/AML Examination Manual.

QUESTION NO: 36

At a small community bank, the compliance officer identifies unusual activity on a customer, who with his personal and company accounts, is the bank's largest depositor. The customer's companies have significant balances on their outstanding loans. The compliance officer notices that there is a lot of unusual movements of money between the customer's individual and business accounts. After filing a suspicious transaction report (STR), the compliance officer gets a call from law enforcement indicating that they want the bank to keep the account open while they conduct an investigation into the customer.

How should the compliance officer escalate this information to the board of directors?

A. By providing a copy of the STR to the board

B. By informing the regulator to bring it up with their next meeting with the board

C. By providing a high level summary of the activity and the interactions with law enforcement

D. By providing a copy of the letter from law enforcement asking the bank to keep the account open.

ANSWER: C

Explanation:

The compliance officer should escalate the matter to the board by providing a high-level summary of the risk, the unusual activity observed, and the fact and nature of communications with law enforcement—without disclosing the existence or contents of the filed STR. Board oversight expectations in AML programs include being informed about significant

compliance risks, material investigations, and management's response (including account-risk decisions and any law-enforcement requests), but STR/SAR confidentiality rules generally prohibit sharing the report itself or revealing that a report was filed to unauthorized parties. In practice, boards receive aggregated or sanitized reporting (e.g., trends, significant cases, and management actions) that enables governance and decision-making while maintaining required confidentiality. A concise briefing should cover: the customer relationship risk (including concentration/credit exposure), observed transactional red flags, steps taken (enhanced monitoring, EDD, risk-rating changes), the law enforcement request to maintain the relationship, and proposed controls and next steps (e.g., documented rationale, ongoing monitoring cadence, legal/regulatory consultation). This approach supports effective governance and avoids inadvertent "tipping off" or improper disclosure of STR/SAR information.

References: FinCEN SAR Confidentiality; FFIEC BSA/AML Manual – Board of Directors and Senior Management

QUESTION NO: 37

One key aspect of the Office of Foreign Assets Control's extraterritorial reach includes the blocking of certain non-United States initiated transactions for or through the United States (U.S.) for benefit of a restricted person or entity.

Under which three circumstances are U.S. banks required to block transactions? (Choose three.)

A. The transactions are to, or go through, a blocked entity

B. Those that are by, or on behalf of, a blocked individual or entity

C. Those that are by or on behalf of a blocked individual and a licensed entity

D. Those that are in connection with a transaction in which a blocked individual or entity has an interest

E. Those that are in connection with a transaction in which a blocked individual or entity has no interest

ANSWER: A B D

Explanation:

U.S. banks must block (freeze) property and interests in property of sanctioned parties when the transaction involves a blocked person or blocked property and comes within U.S. jurisdiction (including being processed "for or through" the United States). In practice, this means a bank must block funds when the payment is to, from, or routed through a blocked entity, because the blocked party's property interest is present in the transaction flow. Banks must also block when a transaction is conducted by, or on behalf of, a blocked individual or entity (including situations where an intermediary is acting for the blocked party), since the blocked party retains an interest in the funds or benefit being transferred. Finally, blocking is required when the transaction is connected to any dealing in which a blocked person has an interest—even if the blocked person is not the originator or beneficiary—because OFAC's "property and interests in property" standard captures direct and indirect interests. These blocking obligations are core to OFAC compliance programs and are distinct from "rejecting" transactions, which applies in some sanctions programs but does not substitute for blocking when a blocked person's interest exists. See OFAC's guidance on blocked property and compliance expectations: https://ofac.treasury.gov/faqs/topic/1621 and https://ofac.treasury.gov/compliance.

QUESTION NO: 38

The new compliance officer has reviewed the bank's anti-money laundering training program. The program consists of online training for all new employees within 30 days of hire date and annual refresher training to all employees. In addition, there is specialized training for areas that deal with higher risk products and customers.

Over the last year, there have been no regulatory changes and no new products or services have been introduced. The compliance officer wants to propose to the board of directors that the annual refresher training is still current and can be delivered unchanged to all employees.

Which two critical pieces of information could be missed by taking this approach? (Choose two.)

A. Any new trends, developments, or risks

B. Results of the previous year's risk assessment

C. Changes to internal policies, procedures, and processes

D. Links to enforcement actions identifying violations in other financial institutions

ANSWER: A B C

Explanation:

Even when there are no regulatory changes and no new products, AML training should be refreshed to reflect the institution's evolving risk profile and operational reality. A key input is the results of the previous year's risk assessment, because it may show shifts in customer base, delivery channels, geographies, transaction patterns, or control effectiveness that require updated examples, red flags, and escalation expectations in training. Another critical input is changes to internal policies, procedures, and processes. Institutions frequently update monitoring rules, alert triage steps, SAR decisioning workflows, recordkeeping, or onboarding/EDD standards based on audit findings, model tuning, staffing changes, or lessons learned from investigations—none of which require a regulatory change to be material for employees. If annual training is delivered unchanged, staff may not learn the current "how we do it here" requirements or the most relevant risks the bank is actually facing, which undermines the effectiveness of the AML program and the board's oversight responsibilities. This aligns with regulatory expectations that training be ongoing and tailored to roles and risks, and updated as needed based on risk assessments and program changes.

References: FFIEC BSA/AML Examination Manual – Training; FinCEN Guidance (AML program expectations and updates)

QUESTION NO: 39

The AML compliance officer of a financial institution (FI) has been advised that the institution is being investigated by the country's financial intelligence unit (FIU). What should the AML compliance officer do? (Select Two.)

A. inform senior leadership and the board of the investigation.

B. Share investigation results with other FIs to help them prepare.

C. Monitor the progress of the investigation by keeping clear records.

D. Send an informative communication to all employees about the investigation.

E. Provide all information to the FIU as soon as possible to avoid delays.

ANSWER: A C E

Explanation:

When a financial institution is under review by a financial intelligence unit, the AML compliance officer's priority is to ensure appropriate governance oversight and disciplined case management. Informing senior leadership and the board of the investigation is a core expectation because FIU inquiries can create significant legal, regulatory, reputational, and operational risk; senior management and the board must be positioned to allocate resources, engage counsel as needed, and oversee remediation. In parallel, monitoring the progress of the investigation by keeping clear records is essential to demonstrate cooperation, maintain an audit trail, and ensure timely, accurate responses to requests. Good recordkeeping should track what was requested, what was produced, when it was produced, applicable deadlines, extensions, and any follow-up communications. This approach aligns with widely accepted AML governance practices: escalation to appropriate oversight bodies and maintaining documentation that supports transparency, accountability, and effective coordination with competent authorities. These actions also help the institution avoid inconsistent messaging, missed deadlines, or incomplete productions that can worsen regulatory outcomes. See general FIU context and expectations at Egmont Group and FATF guidance on cooperation and competent authorities at FATF Recommendations.

QUESTION NO: 40

OFAC-issued regulations apply to which entities? (Choose two.)

A. Intermediaries transacting with US banks

B. Foreign banks with US customers

C. Foreign subsidiaries of US banks

D. US branches of a foreign bank

E. Foreign import-export companies

ANSWER: C D

Explanation:

OFAC sanctions regulations generally apply to "U.S. persons," which includes U.S. citizens and permanent residents wherever located, entities organized under U.S. law (including their foreign branches), and any person or entity physically present in the United States. In the banking context, this means a U.S. branch of a foreign bank is subject to OFAC because it operates in the United States and is therefore a U.S. person for OFAC compliance purposes while in the U.S. It also means foreign subsidiaries of U.S. banks can be subject to OFAC requirements depending on the specific sanctions program and the nature of the U.S. ownership/control and applicable "U.S. person" definitions; in practice, U.S. financial groups commonly extend OFAC controls to foreign subsidiaries to ensure groupwide compliance and to meet program-specific requirements (for example, certain Cuba- and Iran-related authorities historically reached some foreign entities owned/controlled by U.S. persons). Accordingly, the best answers are the U.S. branches of a foreign bank and foreign subsidiaries of U.S. banks as entities to which OFAC regulations can apply in the financial services setting.

References: OFAC FAQs – "U.S. person"; FFIEC BSA/AML Manual – OFAC

QUESTION NO: 41

Which statement identifies one of the duties of a government Financial Intelligence Unit?

A. It serves as the central agency for the receipt of disclosures filed by reporting entities.

B. It administers and enforces economic and trade sanctions based on a government's foreign policy and national security goals.

C. It supervises and regulates banking institutions to ensure the safety and soundness of the nation's banking and financial system.

D. It prosecutes suspected money launderers and terrorist financiers based on financial institution suspicious transaction report filings.

ANSWER: A

Explanation:

A core duty of a government Financial Intelligence Unit is to act as the national "central agency" for receiving (and typically analyzing and disseminating) financial disclosures such as suspicious transaction/activity reports submitted by reporting entities. This is consistent with the widely accepted FIU model described by the Egmont Group and reflected in FATF standards: reporting entities submit STRs/SARs to the FIU, which then develops financial intelligence and shares it with competent authorities (e.g., law enforcement) when appropriate. Importantly, FIUs generally do not prosecute cases themselves; prosecution is a function of prosecutorial authorities, while prudential supervision is performed by banking regulators, and sanctions administration is typically handled by a sanctions authority (often a finance ministry/treasury or foreign affairs body). Therefore, the statement about serving as the central agency for the receipt of disclosures filed by reporting entities correctly identifies an FIU duty.

References: FATF Recommendations (see Recommendation 29 on FIUs); Egmont Group – About.

QUESTION NO: 42

Typical events to identify and investigate potential AML activities include: (Select Three.)

A. blocked transactions involving individuals included in the Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons List.

B. internal tips from employees of the bank about potential suspicious activity.

C. alerts triggered by the automated AML monitoring system.

D. subpoenas requesting information for civil cases.

E. requests from law enforcement agencies.

F. accounts going to dormant status.

ANSWER: A B C

Explanation:

Typical AML "events" that should be identified, triaged, and investigated are those that reliably indicate potential sanctions exposure or suspicious activity requiring escalation under an institution's AML program. Blocked transactions involving parties on the Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons List are a classic trigger because sanctions screening hits can require immediate interdiction, blocking/rejecting decisions, and follow-on investigation/documentation. Internal tips from employees are also a common and important trigger; staff may observe unusual customer behavior, inconsistent explanations, or operational red flags that automated systems miss, and AML programs are expected to have channels to capture and assess such referrals. Alerts triggered by the automated AML monitoring system are a core detection mechanism in most financial institutions; transaction monitoring scenarios and rules generate alerts that must be reviewed, dispositioned, and, where warranted, investigated further and potentially reported. These three event types align with standard CAMS expectations around sources of detection: sanctions screening, internal referrals, and automated transaction monitoring. See OFAC sanctions program and SDN list context at Treasury/OFAC SDN resources and FinCEN's overview of SAR expectations and suspicious activity reporting at FinCEN Guidance.

QUESTION NO: 43

A bank operates in multiple countries and offers a variety of products and services. The compliance officer recently joined the bank and wants to better understand the inherent level of anti-money laundering risk across the entire organization.

Which two factors should be considered? (Choose two.)

A. The Transaction Monitoring program

B. The Customer Due Diligence program

C. Countries that the bank operates in

D. Products and services offered by the bank

ANSWER: C D

Explanation:

To understand an organization's *inherent* AML risk, the compliance officer should focus on the bank's underlying exposure before considering the strength of controls. Two core drivers of inherent risk are the jurisdictions involved and the nature of the products/services offered. Countries that the bank operates in matter because different jurisdictions present different levels of money laundering, corruption, sanctions, and regulatory risk; operating in or serving higher-risk jurisdictions increases baseline exposure regardless of how good the control framework is. Products and services offered by the bank are also central because certain offerings (for example, private banking, correspondent banking, trade finance, cash-intensive services, or products enabling rapid movement of funds) inherently create more opportunity for misuse and layering. These factors are standard inputs in an enterprise-wide AML risk assessment and are evaluated alongside other inherent-risk dimensions (such as customer types and delivery channels) to form a holistic view of risk exposure. Control programs like transaction monitoring and customer due diligence are important, but they are typically assessed as mitigating controls rather than inherent-risk factors.

References: FATF – Risk-Based Approach; FFIEC BSA/AML Examination Manual – Risk Assessment

QUESTION NO: 44

A bank employee recently opened an account for a new restaurant. Daily cash deposits over a threemonth period are close to $9,500.

What are two red flags that indicate possible money laundering or terrorist financing? (Choose two.)

A. The restaurant is located in a different city

B. The daily cash deposits are so close in amount

C. It is a new account that has daily cash deposits

D. The new account demonstrates a steady flow of income

ANSWER: B C

Explanation:

Two key red flags here are the repeated cash deposits that are consistently just below a common reporting threshold and the pattern of frequent cash activity immediately after account opening. Daily deposits close to $9,500 over an extended period can indicate structuring (also called “smurfing”), where transactions are deliberately kept below the Currency Transaction Report threshold (e.g., $10,000 in the U.S.) to evade reporting and detection. A second red flag is that this is a newly opened account showing daily cash deposits right away; rapid, high-frequency cash activity early in the relationship can be inconsistent with what the institution reasonably expects for a new customer absent corroborating business rationale, and it warrants enhanced scrutiny and potential escalation. In CAMS-style analysis, the focus is on unusual patterns and intent to avoid controls, not simply that a business has revenue. A “steady flow of income” by itself is not inherently suspicious; the suspicious element is the near-threshold, repetitive cash pattern and the immediate, frequent cash activity in a new relationship. These are classic transaction-monitoring indicators that should trigger review, possible customer outreach, and consideration of SAR/STR filing depending on findings.

References: FinCEN guidance on structuring; FFIEC BSA/AML Examination Manual (Suspicious Activity Reporting)

QUESTION NO: 45

Which trading pattern may be indicative of money laundering in capital markets?

A. Free of payment asset transfer

B. Remittance of a round dollar amount

C. Trading on an account

D. Transacting with multiple counterparties

ANSWER: D

Explanation:

Transacting with multiple counterparties may be indicative of money laundering in capital markets because it can be used to obscure beneficial ownership, complicate audit trails, and create layering through a web of trades and settlements. In securities markets, layering often involves spreading activity across numerous counterparties (and sometimes multiple intermediaries) to make it difficult to link the origin of funds to the ultimate recipient, especially when combined with rapid in-and-out trading, cross-border counterparties, or accounts that appear unrelated but trade in a coordinated way. This pattern can also facilitate the movement of value without an obvious economic rationale, particularly when the customer repeatedly routes transactions through different counterparties rather than using a stable set consistent with their stated strategy. FATF’s work on money laundering and terrorist financing in the securities sector highlights that complex trading chains and the use of multiple parties can be a red flag because they increase opacity and can be consistent with layering typologies. Firms should therefore treat unusual counterparty dispersion—relative to the customer profile, expected trading behavior, and product risk—as a potential indicator requiring enhanced review and, where appropriate, escalation and reporting. See

FATF's sector report: FATF – ML and TF in the Securities Sector and the IOSCO principles context for securities supervision: IOSCO Objectives and Principles of Securities Regulation.

QUESTION NO: 46

Which two steps should a financial institution take when it receives a law enforcement request to keep an account open that may be associated with suspicious or criminal activity? (Choose two.)

A. File a suspicious transaction report on the account owner(s)

B. Maintain account records for at least five years after the request expires

C. Ask for a written request from the law enforcement agency that defines the duration

D. Stop filing suspicious transaction reports because law enforcement will be monitoring the account

ANSWER: B C

Explanation:

When law enforcement asks a financial institution to keep an account open (often to support an investigation), best practice and FinCEN guidance emphasize two core controls: obtain the request in writing with clear parameters, and ensure appropriate record retention. A written request should identify the requesting agency, specify the account(s) involved, and define the duration (including any renewal/extension process). This protects the institution by documenting the legal basis and scope of the request and helps ensure the institution can manage operational and risk decisions consistently over time. In addition, the institution should retain records related to the request and the account activity for the required period—commonly at least five years—so that the institution can evidence compliance and support any later investigative or regulatory needs. These steps align with FinCEN's guidance on law enforcement requests to maintain accounts and with general BSA/AML recordkeeping expectations. See FinCEN's guidance here: https://www.fincen.gov/resources/statutes-regulations/guidance/requests-law-enforcement-financial-institutions-maintain and FinCEN's BSA recordkeeping overview here: https://www.fincen.gov/resources/statutes-regulations/bsa.

QUESTION NO: 47

What action should a bank CEO's assistant take when the bank CEO expenses large sums of money to a charitable organization run by the bank CEO's direct family member?

A. Report the actions to the Executive Board of the bank.

B. Meet with the bank CEO to learn why the donations are being made.

C. Investigate the charitable organization's relationship with the bank CEO.

D. Submit the concern anonymously to the bank's internal Compliance Hotline.

ANSWER: D

Explanation:

Submitting the concern anonymously to the bank's internal Compliance Hotline is the most appropriate action because it routes a potential conflict-of-interest and possible misuse of corporate funds into the bank's established escalation and investigation process, while protecting the employee from retaliation or undue pressure. In AML/ethics best practice, employees who observe potentially improper activity—especially involving senior management—should not attempt to investigate themselves or confront the subject directly. Instead, they should use formal reporting channels (whistleblowing/hotline, compliance, ethics office) so the matter can be assessed independently, documented, and handled under governance controls (e.g., conflicts-of-interest review, gifts/charitable contributions policy, potential fraud review, and any required regulatory reporting). This approach aligns with the "three lines" concept and ACAMS-style expectations that staff escalate suspicions through internal controls rather than conducting ad hoc inquiries. It also recognizes the heightened

risk when transactions involve a senior executive and a close family member, where independence and confidentiality are critical to ensure an unbiased review.

References: OCC – Corporate Governance; SEC – Whistleblower Program (principles of protected reporting).

QUESTION NO: 48

Which are common types of economic sanctions? (Choose three.)

A. Targeted sanctions

B. Technological sanctions

C. SWIFT network sanctions

D. Sectoral sanctions

E. Supervisory sanctions

F. Comprehensive sanction

ANSWER: A D F

Explanation:

Commonly recognized categories of economic sanctions in AML/sanctions compliance include targeted (or “smart”) sanctions, comprehensive (country-wide) sanctions, and sectoral sanctions. Targeted sanctions focus restrictions on specific persons, entities, vessels, aircraft, or activities—typically implemented through designation/listing programs (e.g., asset freezes and prohibitions on dealing). Comprehensive sanctions broadly restrict trade, financial flows, and other dealings with an entire jurisdiction (often with limited exceptions such as humanitarian authorizations). Sectoral sanctions restrict certain types of transactions (e.g., specific financing terms, debt/equity dealings, or services) involving defined sectors of an economy (such as energy, defense, or financial services), rather than imposing a full embargo.

These three types are widely used by major sanctions authorities and are core concepts tested in CAMS-style questions because they drive screening, customer/transaction due diligence, and controls design (e.g., list screening for targeted sanctions, jurisdictional controls for comprehensive sanctions, and product/transaction-attribute controls for sectoral sanctions). For a practical overview of sanctions types and how they are applied, see the Council on Foreign Relations backgrounder (https://www.cfr.org/backgrounder/what-are-economic-sanctions) and OFAC’s sanctions program descriptions (https://ofac.treasury.gov/sanctions-programs-and-country-information).

QUESTION NO: 49

How does the Asian/Pacific Financial Action Task Force -Style Regional Body help its members implement recommendations from the FATF? (Select Two.)

A. Promotes laws that allow judicial challenges to seizure orders by an administrative body

B. Endorses regulations that define money laundering based on the model laws issued by the respective member states

C. Facilitates the adoption and implementation of internationally accepted AMI measures by member jurisdictions

D. Encourages cooperative AML efforts in the region

E. Requires members to maintain lists of regional money laundering and terrorists financing issues relevant to their region

ANSWER: C D

Explanation:

FATF-Style Regional Bodies (FSRBs) such as the Asia/Pacific Group on Money Laundering (APG) support implementation of the FATF Recommendations primarily by driving consistent adoption of international AML/CFT standards and by fostering

regional cooperation. In practice, this includes helping jurisdictions translate FATF standards into effective national frameworks (laws, regulations, supervisory expectations, and operational practices) and promoting convergence with globally accepted measures so that member regimes are aligned with the FATF Recommendations. APG also strengthens implementation through cooperative regional AML/CFT efforts—most notably by facilitating collaboration among members, sharing typologies and best practices, and supporting peer-based mechanisms (including mutual evaluation processes and follow-up) that encourage ongoing improvements and sustained compliance. These functions are central to the role of FSRBs as recognized by FATF and reflected in CAMS-aligned best practices for how international standard setters and their regional bodies promote effective AML/CFT regimes. See FATF's description of FSRBs and their role in promoting implementation and cooperation: https://www.fatf-gafi.org/en/about-fatf/fatf-style-regional-bodies.html and APG's mandate and activities: https://apgml.org/.

QUESTION NO: 50

Which situations would require a financial institution (FI) to update its ML/TF risk assessment? (Choose two.)

A. When new products, services or customer types are introduced

B. When new board members are elected

C. When the AML compliance team hires new employees

D. When the institution faces a merger or acquisition

E. When opening a sales point in a new location in the same city

ANSWER: A D

Explanation:

An FI should update its ML/TF risk assessment when there is a material change to its inherent risk profile or to the effectiveness/coverage of its controls. Introducing new products, services, delivery channels, or customer types can change exposure to different typologies (for example, higher-risk non-face-to-face onboarding, new payment rails, or new customer segments), so the risk assessment must be refreshed to ensure risks are identified, measured, and mitigated appropriately. Similarly, a merger or acquisition can significantly alter the FI's customer base, geographic footprint, product mix, transaction volumes, and control environment (including integration gaps), all of which are classic triggers for reassessing ML/TF risk and recalibrating controls, monitoring, and resourcing. These triggers align with FATF's risk-based approach expectations that risk assessments are not static and should be kept current as circumstances change, and with common regulatory guidance that risk assessments be updated upon significant business changes. See FATF's risk assessment guidance and the FATF risk-based approach materials for the expectation of ongoing, event-driven updates: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach.html and https://www.fatf-gafi.org/en/publications/Methodsandtrends/National_ML_TF_Risk_Assessment.html.

QUESTION NO: 51

As a result of an audit, a policy exception was identified that had been approved by the compliance officer. The auditor determined that the policy exception is a violation of a regulatory requirement.

What should the auditor do?

A. Advise the compliance officer on how to appropriately respond to policy exceptions.

B. Include the regulatory violation in the audit report and report it to the board of directors.

C. Consult with legal counsel to determine if the approval of the policy exception was acceptable.

D. Include the regulatory violation in the audit report and recommend the compliance officer be subject to disciplinary action by the board of directors.

ANSWER: B

Explanation:

The appropriate action is to document the issue as a regulatory violation in the audit report and ensure it is escalated to the appropriate level of governance, including the board of directors (or an audit committee acting on the board's behalf). In AML/financial crime compliance, internal audit's role is to provide independent assurance over the effectiveness of governance, risk management, and controls, and to report significant control failures and compliance breaches through formal audit reporting and escalation channels. A policy "exception" cannot override a regulatory requirement; once audit concludes a breach exists, it must be reported as an audit finding so management and the board can drive timely remediation, assess regulatory impact, and determine whether self-reporting to regulators is required. This approach preserves audit independence and avoids audit taking on management responsibilities (such as coaching compliance on how to handle exceptions) or making HR/disciplinary recommendations, which are typically outside audit's mandate. Escalation to the board is consistent with widely accepted internal audit standards for communicating significant risk exposures and control issues to those charged with governance. See the IIA's International Standards for the Professional Practice of Internal Auditing (communication of results) and Basel's principles on internal audit's role in banks.

References: https://www.theiia.org/en/standards/ ; https://www.bis.org/publ/bcbs223.htm

QUESTION NO: 52

What does the Financial Action Task Force (FATF) urge its members and all other jurisdictions to do when a jurisdiction is identified as having lax anti-money laundering / counter financing of terrorism controls?

A. Apply counter-measures to that jurisdiction

B. Consider customers from that jurisdiction as high risk

C. Cease doing business with that jurisdiction immediately

D. Apply economic sanctions until otherwise notified by FATF

ANSWER: A

Explanation:

When FATF identifies a jurisdiction as having serious strategic AML/CFT deficiencies (commonly reflected in FATF "Public Statements" for high-risk jurisdictions), it urges members and other jurisdictions to apply counter-measures to protect the international financial system. In FATF usage, "counter-measures" are enhanced, jurisdiction-level risk mitigants that go beyond routine enhanced due diligence and are intended to limit exposure to the risks emanating from that jurisdiction. These measures can include, depending on the FATF call, actions such as increased supervisory examination, enhanced reporting requirements, restrictions on establishing branches/subsidiaries, or other proportionate steps designed to reduce ML/TF risk. This is distinct from automatic sanctions or a blanket requirement to exit all relationships; FATF's call is specifically framed as applying counter-measures (or, in some cases, applying enhanced due diligence) in line with the public statement for that jurisdiction. The key point is that FATF is directing jurisdictions to take protective action at the country-risk level, consistent with the FATF Recommendations and the specific language of the applicable public statement.

References: FATF – High-risk and other monitored jurisdictions; FATF Recommendations.

QUESTION NO: 53

What must be materially true regarding transactions for United States (U.S.) sanctions laws to have jurisdiction?

A. Transactions are traced to illegal proceeds

B. Transactions are processed by a U.S. person

C. Transactions are stripped of beneficial owner information

D. Transactions are identified as proceeds of foreign corruption

ANSWER: B

Explanation:

For U.S. sanctions laws to have jurisdiction over a transaction, there must be a U.S. nexus—most commonly that the transaction is conducted by, through, or involving a "U.S. person" (e.g., U.S. citizens/permanent residents, entities organized under U.S. law and their foreign branches, and any person physically in the United States). In practice, this includes transactions processed by U.S. financial institutions, cleared through the U.S. financial system, or otherwise handled by U.S. persons acting in their capacity. This jurisdictional hook is central to OFAC's enforcement framework: if a U.S. person is involved in processing, approving, facilitating, or otherwise dealing in the transaction, U.S. sanctions prohibitions can apply (subject to the specific sanctions program, general licenses, and authorizations). This is why non-U.S. parties can still face blocked/rejected payments when a payment message routes through a U.S. bank or a U.S. branch, or when a U.S. person provides services connected to the transaction. OFAC's published guidance and FAQs emphasize the importance of U.S.-person involvement and U.S.-system touchpoints as the basis for U.S. jurisdiction in many sanctions scenarios.

References: https://ofac.treasury.gov/faqs, https://ofac.treasury.gov/sanctions-programs-and-country-information

QUESTION NO: 54

The compliance officer for a private bank has been tasked with reviewing the procedure for authorized signatories on customer accounts to ensure it is in line with relevant Wolfsberg Anti-Money Laundering Principles for Private Banking.

Which three statements from the procedure are in line with Wolfsberg? (Choose three.)

A. Where the Authorized Signatory is not a lawyer or accountant, due diligence as to the source of funds and wealth of the Authorized Signatory should be undertaken.

B. The responsible private banker must establish the identity of a holder of general powers over an account (e.g. a signatory for the account) and, as appropriate, verify that identity.

C. Where due diligence has been satisfactorily completed on all authorized signers, the responsible private banker may reduce the due diligence performed on the account holder and/or beneficial owner.

D. The responsible private banker must obtain the necessary documentation establishing the authorized signer's authority to act on behalf of the account holder or beneficial owner (e.g. a Power of Attorney).

E. If an individual has signing authority over an account but does not act on a professional basis as a manager of funds, the responsible private banker must understand and document the relationship between that authorized signer, the account holder, and, if different, the beneficial owner of the account.

ANSWER: B D E

Explanation:

Under the Wolfsberg Anti-Money Laundering Principles for Private Banking, authorized signatories (including holders of powers of attorney or other mandate arrangements) are treated as relevant parties whose identity and authority must be appropriately established. In practice, this means the private banker should identify the person who has general powers over the account and, where appropriate, verify that identity using reliable, independent source documents. Wolfsberg also expects the bank to obtain and retain documentation evidencing the signatory's authority to act (for example, a power of attorney, mandate, board resolution, or equivalent), because understanding "who can move funds" is central to controlling misuse of accounts.

In addition, where a signatory is not acting in a professional capacity as an intermediary or funds manager, Wolfsberg emphasizes understanding and documenting the relationship between the signatory, the account holder, and (if different) the beneficial owner. This relationship context helps detect red flags such as nominee arrangements, hidden beneficial ownership, or undue influence, and supports ongoing monitoring and escalation when activity is inconsistent with the stated relationship.

References: Wolfsberg FAQs on Intermediaries (May 2012); Wolfsberg AML Principles for Private Banking (2012).

QUESTION NO: 55

Which product type is subject to US extra jurisdictional reach over non-US banks and non-US persons under the USA PATRIOT Act?

A. Correspondent banking

B. Commercial lending

C. Trade finance

D. Private banking

ANSWER: A

Explanation:

Correspondent banking is the product type most directly associated with the USA PATRIOT Act's extraterritorial (extra-jurisdictional) reach over non-U.S. banks and non-U.S. persons. A core focus of Title III of the USA PATRIOT Act is preventing foreign institutions from accessing the U.S. financial system anonymously or indirectly, and correspondent accounts are the primary channel through which many foreign banks obtain U.S. dollar clearing and other U.S. financial services. The Act and implementing rules impose specific obligations and enforcement tools tied to correspondent accounts, including enhanced due diligence requirements for certain foreign correspondent accounts and special measures that can restrict or prohibit maintaining correspondent accounts for designated institutions or jurisdictions. In practice, this means non-U.S. banks and non-U.S. persons can be impacted by U.S. AML expectations and enforcement when they use, maintain, or transact through U.S.-linked correspondent relationships, even if much of the activity occurs outside the United States. This is why CAMS materials commonly highlight correspondent banking as a key example of the PATRIOT Act's extended reach beyond U.S. borders.

References: FinCEN – USA PATRIOT Act; eCFR – 31 CFR 1010.610 (Due diligence for correspondent accounts)

QUESTION NO: 56

Which transaction monitoring processes would alert a bank for red flag activity?

A. A client who does not typically make extravagant credit card purchases books an airline ticket on a travel website.

B. The company has a name that is similar to that of a company whose directors are named on the bank's internal blacklist.

C. A client makes a prepayment on their credit card and a week later makes multiple cash withdrawals using an automated teller machine (ATM) in a foreign country.

D. A charity account receives multiple electronic transfers and then sends a wire transfer to a higher-risk country.

ANSWER: C

Explanation:

"A client makes a prepayment on their credit card and a week later makes multiple cash withdrawals using an automated teller machine (ATM) in a foreign country." is the clearest example of activity that transaction monitoring is designed to detect and alert on. Transaction monitoring looks for unusual patterns versus a customer's expected behavior, including rapid movement from a funding event into cash access, especially when it involves foreign geographies. A credit card prepayment (which can create available credit) followed shortly by multiple ATM cash withdrawals abroad can indicate attempts to convert funds into cash quickly, potentially obscuring source of funds and complicating traceability. This kind of pattern is commonly treated as a behavioral red flag because it combines atypical account behavior (prepayment) with higher-risk channel and location factors (cash withdrawals and foreign country usage), which are standard inputs to monitoring scenarios and alert rules. In practice, banks tune scenarios to detect spikes in cash advances/ATM withdrawals, unusual foreign usage, and sudden changes in payment behavior, then escalate alerts for review and potential SAR/STR filing where warranted. See FATF guidance on risk-based controls and monitoring (https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html) and the U.S. FFIEC BSA/AML Examination Manual discussion of monitoring and suspicious activity identification (https://bsaaml.ffiec.gov/manual).

QUESTION NO: 57

Which measure to mitigate risk does the Basel Committee's Customer Due Diligence Principles suggest banks apply when accepting business from non-face-to-face customers?

A. Certification of documents presented

B. Requiring an in person interview with the customer

C. Imposing a limit on permissible account activity for a defined period of time

D. Requiring additional review of account opening documents by senior management

ANSWER: A

Explanation:

The Basel Committee's Customer Due Diligence (CDD) guidance highlights that non-face-to-face onboarding increases impersonation and identity-fraud risk, so banks should apply compensating controls that strengthen the reliability of identification and verification. A core, practical mitigation measure explicitly referenced in Basel CDD-related guidance is obtaining appropriately certified copies of identification documents (for example, certification by a suitable authority such as a notary, regulated financial institution, or other trusted certifier, depending on local law and the bank's policies). This control helps the bank gain greater assurance that the documents used to establish identity are genuine and belong to the customer, partially offsetting the absence of physical presence. In CAMS-aligned best practice, this measure is typically combined with other non-face-to-face safeguards (e.g., independent verification, trusted digital ID solutions, or additional authentication), but the question asks for a specific measure suggested by the Basel Committee for non-face-to-face customers. Certification of documents presented is therefore the most directly aligned choice with the Basel Committee's recommended risk-mitigation approach for remote relationships.

References: Basel Committee on Banking Supervision – Customer due diligence for banks; FATF Recommendations (CDD framework supporting enhanced measures for higher-risk scenarios).

QUESTION NO: 58

A financial institution (FI) is being investigated for possible money laundering. When cooperating with law enforcement agencies, which additional steps should the FI ensure are taken? (Choose two.)

A. Centralized control is maintained over all requests and responses to ensure completeness and timely responses.

B. Make employees, including corporate officers, unavailable for interviews and refuse documents upon receipt of a subpoena.

C. Subpoenas and other information requests should be reviewed by senior management and an investigations group or counsel.

D. Address the document destruction policy to ensure the relevant documents are destroyed.

E. Inquiries from the media are not answered directly, but rather are addressed by replying, "No comment."

ANSWER: A C

Explanation:

When a financial institution is under investigation and cooperating with law enforcement, it should implement strong governance around how requests are received, triaged, fulfilled, and documented. Maintaining centralized control over all requests and responses helps ensure consistency, completeness, appropriate approvals, and timely production—reducing the risk of missed deadlines, inconsistent statements, or inadvertent disclosure of privileged or nonresponsive information. In parallel, subpoenas and other information requests should be reviewed by senior management and an investigations group or counsel to confirm scope, preserve legal privilege where applicable, coordinate with the AML/financial crimes function, and ensure proper legal holds are issued so relevant records are retained and produced appropriately.

These steps align with common best practices for responding to law enforcement process (e.g., subpoenas, summonses, production orders) and for managing regulatory/legal risk during investigations. They also support defensible decision-making and auditability, which is critical if the institution's cooperation and responsiveness are later scrutinized by prosecutors or regulators. For additional context on subpoena response expectations and record retention/production considerations, see the U.S. DOJ Justice Manual guidance on subpoenas and compulsory process (https://www.justice.gov/jm/jm-9-11000-grand-jury) and FinCEN's overview of the BSA framework and compliance expectations (https://www.fincen.gov/resources/statutes-regulations/bank-secrecy-act).