a.k.a dumpsqueen.com

Certified Anti-Money Laundering Specialist (6th Edition)

ACAMS CAMS

Version Demo

Total Demo Questions: 90

Total Premium Questions: 904

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Risks and Methods of Money Laundering and Terrorist Financing	229
Topic 2, International AML/CFT Compliance Standards	292
Topic 3, AML/CFT Compliance Programs	270
Topic 4, Conducting or Supporting the AML/CFT Investigation	113
Total	904

QUESTION NO: 1

A compliance officer learns from an Information Technology (IT) source of a potential new financial service being discussed by the new product approval committee.

What is the correct next course of action?

A. Request that the new product approval committee include the compliance officer.

B. Go to the board of directors and try to shut the new service down immediately because the committee did not communicate with the compliance officer.

C. Get as much information as possible from the source so that potential risks can be researched and a report prepared and presented to the head of marketing.

D. Start initial research into potential risks but wait until notified that the service has been approved by the committee before initiating extensive research.

ANSWER: A

Explanation:

Request that the new product approval committee include the compliance officer. A financial institution's new-product governance process should engage Compliance at the earliest practical stage, before a product or service is approved or implemented. This enables the compliance function to identify and assess financial-crime risks arising from the proposed service, customer base, delivery channel, geographic exposure, transaction characteristics, and third-party dependencies. Compliance can then ensure that appropriate controls, policies, procedures, staffing, training, customer due diligence, sanctions screening, and transaction-monitoring capabilities are designed and operational before launch.

Formal inclusion is important because it makes AML/CTF review a documented, repeatable governance requirement rather than an informal response triggered by information obtained from another department. It also supports independent compliance oversight and allows risk acceptance decisions, mitigating controls, and relevant approvals to be recorded clearly. This proactive approach reflects the risk-based framework expected of regulated institutions and helps ensure that the institution's BSA/AML program remains appropriately tailored as products and services change. The FFIEC manual discusses the need for a BSA/AML compliance program commensurate with an institution's risk profile, while FATF's risk-based approach calls for identifying, assessing, and mitigating money-laundering and terrorist-financing risks. See the FFIEC BSA/AML Examination Manual and FATF Recommendations.

QUESTION NO: 2

A basic principle of the Egmont Group is to:

A. Publish standards for reporting suspicions

B. Facilitate the organization of regulatory authorities

C. Publish decisions taken on international investigations

D. Arrange information-sharing protocols between Financial Intelligence Units (FIUs)

ANSWER: D

Explanation:

"Arrange information-sharing protocols between Financial Intelligence Units (FIUs)" is correct because the Egmont Group is a global network created to enable and enhance cooperation among FIUs. Its central purpose is the secure, timely, and lawful exchange of financial intelligence relevant to money laundering, associated predicate offences, and terrorist financing. This cooperation is particularly important where suspicious activity, funds, entities, or beneficial owners span several jurisdictions and no single FIU holds the full intelligence picture.

The Egmont Group supports this function through principles for FIU-to-FIU cooperation and secure communication arrangements, notably the Egmont Secure Web. Information exchanged is handled subject to confidentiality safeguards, the supplying FIU's conditions on use and dissemination, and applicable domestic law. These protocols help FIUs request and provide intelligence efficiently while protecting sensitive data and ongoing operational work. The Group's charter expressly identifies the promotion and systematization of information exchange among FIUs as a core objective. This role also aligns with the international standard requiring FIUs to be able to exchange information with foreign counterparts rapidly, constructively, and securely. See the [Egmont Group Charter] and [FATF Recommendation 29].

QUESTION NO: 3

Which collective body of Financial Intelligence Units (FIUs) was formed with an objective to improve Information exchange and sharing mechanisms among member FIUs as well as to support its members by enhancing their capabilities'?

A. The Organisation for Economic Co-operation and Development (OECD)

B. The Egmont Group

C. The Wolfsberg Group

D. The International Monetary Fund (IMF)

ANSWER: B

Explanation:

The Egmont Group is correct. It is the global network of Financial Intelligence Units (FIUs), created to provide a secure and effective framework through which FIUs can exchange financial intelligence and cooperate on money laundering, terrorist financing, and associated predicate offenses. Its core purpose includes improving information exchange among member FIUs, particularly through the secure Egmont Secure Web, and strengthening members' operational capabilities through training, technical assistance, and shared expertise. This cooperative structure helps FIUs develop the practical capacity to receive, analyze, and disseminate suspicious transaction information while enabling timely cross-border intelligence sharing under applicable domestic laws and confidentiality safeguards. The Group's membership principles and support activities promote common standards and effective international cooperation, both of which are central to an FIU's role in an effective anti-money laundering and counter-terrorist financing regime. The Egmont Group describes its mission as facilitating and prompting the exchange of information, knowledge, and cooperation among FIUs worldwide. See the [Egmont Group's description of its work] and the FATF's guidance on [Financial Intelligence Units under Recommendation 29].

QUESTION NO: 4

A law firm is involved in setting up complex offshore corporate structures for a client with minimal documentation of the source of funds. The firm does not question the client's transactions or report any suspicious activity.

What is the primary money laundering risk associated with this behavior by the law firm?

A. The law firm is avoiding fees by minimizing documentation for clients in high-risk jurisdictions

B. The law firm is engaging in aggressive tax planning to help the client avoid legal taxes

C. The law firm is providing routine legal services that include creating complex legal structures, and no further scrutiny is required

D. The law firm is acting as a gatekeeper, facilitating the movement and concealment of illicit funds through complex corporate structures

ANSWER: D

Explanation:

The law firm is acting as a gatekeeper, facilitating the movement and concealment of illicit funds through complex corporate structures. Legal professionals may provide legitimate services involving the creation, purchase, or management of companies, trusts, and other legal arrangements. However, those services can also be exploited to distance criminal proceeds from their source. In this scenario, the use of complex offshore entities combined with minimal source-of-funds documentation creates a substantial risk that ownership, control, and the origin of assets are being obscured. The absence of meaningful inquiry into unusual transactions or suspicious activity further enables illicit funds to be introduced into structures that appear legitimate and then transferred, layered, or held through multiple jurisdictions. FATF identifies lawyers and other independent legal professionals as relevant gatekeepers when they participate in specified activities for clients, including organizing contributions for company creation or managing client money, securities, or other assets. Effective customer due diligence, beneficial-ownership transparency, and suspicious-transaction reporting or escalation obligations, where applicable, are central safeguards against this misuse. See FATF's International Standards on Combating Money Laundering and its risk-based approach guidance for legal professionals.

QUESTION NO: 5

The primary objectives of the Financial Action Task Force (FATF) are to: (Choose two.)

A. evaluate and monitor compliance with the FATF standards and provide recommendations for improvement.

B. assist countries in implementing EU, UN, and regional sanctions regimes.

C. develop and promote international standards to prevent money laundering and terrorist financing.

D. conduct investigations on countries legislations and laws to prevent them from being used for money laundering and terrorist financing.

E. ensure that countries follow its laws to maintain financial stability.

ANSWER: A C

Explanation:

The correct objectives are to develop and promote international standards to prevent money laundering and terrorist financing, and to evaluate and monitor compliance with the FATF standards and provide recommendations for improvement. FATF is an intergovernmental body that establishes the globally recognized FATF Recommendations, which provide a comprehensive framework for combating money laundering, terrorist financing, and proliferation financing. These standards are designed to be implemented through national legal, regulatory, supervisory, and operational measures, while allowing countries to apply a risk-based approach appropriate to their circumstances.

FATF also assesses whether jurisdictions effectively implement these standards. Through mutual evaluations, follow-up processes, and increased monitoring where needed, FATF identifies technical-compliance and effectiveness shortcomings and encourages jurisdictions to address them. This monitoring and recommendation function supports consistent global action and helps protect the integrity of the international financial system. FATF itself does not create binding domestic laws; rather, its influence arises from its standard-setting role, peer review, and the international consequences associated with significant AML/CFT deficiencies. See the FATF overview and the FATF Recommendations.

QUESTION NO: 6

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

A. Declining money supplies

B. Increased sectoral polarization

C. Increased inflation and low economic growth

D. Destabilization of legitimate governments

ANSWER: D

Explanation:

Destabilization of legitimate governments is a profound economic and societal consequence of money laundering because laundering enables criminal organizations to retain, conceal, and deploy the proceeds of crime. Once illicit actors can integrate large sums into the legitimate financial system, they may use that financial power to corrupt public officials, influence political processes, penetrate state-owned or strategically important businesses, and weaken the rule of law. These effects undermine confidence in public institutions and the fairness of markets, impairing a government's capacity to collect revenue, enforce laws, and make policy in the public interest. In more severe circumstances, criminal networks can gain enough economic influence to challenge legitimate governance and institutional stability. The Financial Action Task Force identifies money laundering as a threat to the integrity and stability of financial systems and notes its links to corruption and other serious crime. The International Monetary Fund likewise recognizes that money laundering can damage governance, institutions, and economic development. These governance harms extend beyond an individual financial institution or transaction and demonstrate why effective AML controls are essential to protecting the broader economy and legitimate government authority. See the FATF overview of its work and the IMF AML/CFT resources.

QUESTION NO: 7

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

A. Knowing the goods or services, if identified, do not match the profile of the company or the nature of the financial activity

B. All payments are in smaller amounts below reporting thresholds but are high when aggregated while still being consistent with standard business practices

C. A company regularly conducts large-volume transactions in a medium-risk jurisdiction with longstanding business partners and provides complete documentation and audit trails

D. Insufficient or no information is available to identify originators or beneficiaries of funds transfers through searches or direct inquiries

E. Payments have no stated purpose, do not reference goods or services, or only reference a contract or invoice number

ANSWER: A D E

Explanation:

The indicators "Knowing the goods or services, if identified, do not match the profile of the company or the nature of the financial activity," "Insufficient or no information is available to identify originators or beneficiaries of funds transfers through searches or direct inquiries," and "Payments have no stated purpose, do not reference goods or services, or only reference a contract or invoice number" are well-established warning signs of potential misuse of shell companies and other opaque legal structures. A shell company can be used to create an appearance of legitimate commercial activity while concealing the true purpose of transactions, the source of funds, or the persons who ultimately control or benefit from the activity. Transactions that are inconsistent with a customer's expected business profile may indicate that purported trade is being used to move value rather than support genuine operations. Missing originator or beneficiary information impedes identification of the parties to a transfer and prevents an institution from understanding ownership, control, and transaction purpose. Similarly, vague payment narratives—or references that provide no meaningful commercial detail—can frustrate efforts to establish an economic rationale and may be consistent with layering techniques. FATF identifies inadequate information about parties, unclear transaction purposes, and activity inconsistent with a legal person's business profile as relevant risk indicators in assessing potential misuse of legal persons and arrangements. See FATF beneficial-ownership guidance and FinCEN guidance on suspicious-activity indicators.

QUESTION NO: 8

Which characteristics of trust and company service providers (TCSPs) can potentially make them vulnerable to financial crime? (Select Three.)

A. They may market themselves specifically to criminals

B. Offering nominee directors may increase anonymity by concealing true ownership

C. They do not have to comply with AML regulations in most jurisdictions

D. Selling ready-made, off-the-shelf companies to offshore intermediaries

E. Having minimal face-to-face contact with customers, particularly in offshore arrangements

ANSWER: B D E

Explanation:

Offering nominee directors may increase anonymity by concealing true ownership because nominee arrangements can separate the person appearing in corporate records from the individual who ultimately owns, controls, or benefits from the company. This can complicate customer due diligence, beneficial-ownership identification, and investigation of the source and destination of funds. Selling ready-made, off-the-shelf companies to offshore intermediaries also creates financial-crime exposure: pre-established entities can be transferred quickly and may give users an immediate corporate vehicle through which to open accounts, hold assets, or move funds across jurisdictions. Where the ownership, purpose, and control of such entities are not transparently established, they can facilitate concealment and layering. Having minimal face-to-face contact with customers, particularly in offshore arrangements, can make reliable identity verification and assessment of a customer's stated business purpose more difficult. FATF identifies trust and company service providers as gatekeepers when they form or manage legal persons and arrangements, and its standards require risk-based customer due diligence and beneficial-ownership measures for relevant services. These characteristics are therefore important inherent-risk indicators that require robust controls, verification, and ongoing monitoring. See FATF Recommendations and FATF guidance on concealment of beneficial ownership.

QUESTION NO: 9

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

A. Tailor training and offer regular training to all employees

B. Train outside of daily operations and promote awareness of Compliance

C. Train core AML topics once per year, at a minimum, to relevant employees

D. Use a variety of training methods and provide necessary resources to employees

E. Communicate regularly and measure effectiveness of training

ANSWER: A D E

Explanation:

"Tailor training and offer regular training to all employees," "Use a variety of training methods and provide necessary resources to employees," and "Communicate regularly and measure effectiveness of training" together reflect a sound, risk-based financial-crime training framework. Training must be tailored to employees' roles, responsibilities, exposure to financial-crime risk, and the institution's products, customers, and delivery channels. Regular delivery helps ensure that staff remain able to recognize changing risks, apply internal procedures, and escalate concerns appropriately.

A range of learning methods—such as instructor-led sessions, e-learning, practical case studies, job aids, and targeted refreshers—helps make training accessible and relevant across different functions. Providing supporting resources also enables employees to refer to procedures and warning indicators when needed in their daily work. Ongoing communication reinforces the compliance culture beyond a one-time course. Measuring completion, assessment results, employee feedback, and whether training produces the intended operational outcomes allows the institution to identify gaps and improve the program. This approach supports the expectation that AML/CFT programs provide continuing employee training and are proportionate to the institution's risks. See the FFIEC BSA/AML Manual and FATF Recommendations.

QUESTION NO: 10

Which red flags should be considered prior to establishing a relationship with a third party? (Select Two.)

A. The third party has a lack of anti-corruption compliance clauses in agreements.

B. The third party's amount to be paid for goods and services appears to be reasonable.

C. The third party has requested unusual payment or billing procedures.

D. The third party has a declaration of non-family or business ties with government officials.

E. The third party has sufficient capability to provide the services or goods for which it is being engaged.

ANSWER: A C

Explanation:

The third party has a lack of anti-corruption compliance clauses in agreements and The third party has requested unusual payment or billing procedures are important pre-engagement red flags because they may signal an elevated bribery, corruption, and related financial-crime risk. Effective third-party due diligence should establish whether the prospective intermediary will commit to clear compliance obligations, including adherence to anti-corruption laws, accurate books and records, audit or information rights where appropriate, and termination provisions for misconduct. A resistance to including such protections can indicate that the party is unwilling to operate transparently or be held accountable for its conduct.

Unusual payment or billing procedures require careful review because payment arrangements can be used to disguise the destination, purpose, or beneficiary of improper funds. Examples include requests to pay an account unrelated to the contracting party, payments in a different jurisdiction without a clear business rationale, split or vague invoices, excessive advance payments, cash payments, or payments to entities not involved in delivering the goods or services. The U.S. Department of Justice identifies risk-based third-party management, contractual controls, and payment monitoring as key elements of an effective compliance program. The OECD similarly emphasizes controls over third parties and transactions to prevent foreign bribery. See the U.S. DOJ Evaluation of Corporate Compliance Programs and the OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance.

QUESTION NO: 11

A customer brings $15,000 worth of chips into a casino and plays various games. The customer redeems all the remaining chips and requests a wire transfer of the proceeds to an unrelated third party.

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

A. Customer redeeming all remaining chips

B. Playing various games before cashing out

C. Bringing $15,000 worth of chips into the casino

D. Requesting a wire transfer to an unrelated third party

ANSWER: C D

Explanation:

Bringing $15,000 worth of chips into the casino is a red flag because casino chips are readily transferable instruments of value within the gaming environment. A customer who arrives with a substantial quantity of chips may be attempting to introduce value obtained elsewhere, obscure the original source of funds, or convert chips into a payment instrument that appears to represent legitimate gaming proceeds. The amount also exceeds the $10,000 currency-transaction reporting threshold, making the overall activity particularly important for the casino's monitoring and due-diligence processes.

Requesting a wire transfer to an unrelated third party is also a significant red flag. Third-party payments can create separation between the person conducting the gaming activity and the ultimate recipient of the funds. This may obscure beneficial ownership, facilitate movement of illicit proceeds, or give a transfer the appearance of legitimate casino winnings. Casino AML programs should identify and investigate unusual chip transactions and funds transfers, particularly where the transaction lacks an apparent economic or gaming-related purpose. FinCEN's casino guidance and examination materials emphasize risk-based monitoring, recordkeeping, and suspicious-activity reporting for potentially unusual gaming and funds-transfer activity. See FFIEC BSA/AML Manual: Casinos and FinCEN Guidance.

QUESTION NO: 12

According to the Financial Action Task Force (FATF) Recommendation 22. when involved in customer transactions that include the buying and selling of real estate, real estate professionals are required to apply which customer due diligence (CDD) measures? (Select Two.)

A. Obtaining prior senior manager approval for all related transactions

B. Understanding the purpose of the business relationship

C. Performing adverse media searches on the customer

D. Identifying and verifying the customer's identity

ANSWER: B D

Explanation:

“Understanding the purpose of the business relationship” and “Identifying and verifying the customer's identity” are core customer due diligence measures that apply to real estate agents when they are involved in transactions for clients concerning the buying or selling of real estate. FATF Recommendation 22 extends the applicable Recommendation 10 CDD obligations to designated non-financial businesses and professions, including real estate agents in these circumstances. Recommendation 10 requires institutions and covered professionals to identify the customer and verify that identity using reliable, independent source documents, data, or information. This establishes who is conducting the transaction and supports effective risk assessment. It also requires understanding, and where appropriate obtaining information on, the purpose and intended nature of the business relationship. In a real-estate context, this helps the professional assess whether the transaction is consistent with the customer's stated circumstances and expected activity. These measures are part of a risk-based CDD framework intended to prevent the misuse of property transactions for money laundering or terrorist financing. FATF’s standards state the requirements directly in Recommendation 10 and specify their application to real estate agents in Recommendation 22.

QUESTION NO: 13

An accounting firm opened an account at a bank that is intended to be used as the operational account for the business. After a few months, a comprehensive review of the account was triggered due to unusual activity on the account. Which most likely triggered the review?

A. The account receives international payments that are substantially higher than other fees they typically receive.

B. The account sends monthly donations to several charities that operate in the same communities as the accounting firm.

C. The account receives several payments a day from multiple customers who operate in different industries.

D. The account receives international wires from companies in the Middle East where the accounting firm has several branches.

ANSWER: A

Explanation:

The account receives international payments that are substantially higher than other fees they typically receive. This is the most likely trigger because it represents a material inconsistency with the accounting firm’s expected customer profile and anticipated account activity. An operational account for an accounting practice would ordinarily be expected to receive payments that reasonably correspond to its known services, client base, usual fee levels, and geographic footprint. International incoming payments that are substantially larger than typical fees can indicate that the account is being used for activity outside its stated purpose, including the movement of third-party funds, undisclosed business activity, or possible layering of illicit proceeds.

Ongoing transaction monitoring is intended to identify activity that is unusual relative to information obtained during customer due diligence, including the nature and purpose of the relationship and expected transactions. A significant disparity in payment size is especially relevant because it warrants the bank’s review of payment originators, underlying invoices or contracts, source of funds, and whether the transactions have a credible economic purpose. The review may lead to updated customer due diligence and, where suspicion remains after investigation, consideration of a suspicious activity report. See the FFIEC BSA/AML Manual on ongoing customer due diligence and monitoring and FATF Recommendations.

QUESTION NO: 14

The manager of a bank ' s KYC team discovers that a high-risk customer ' s activity was not reviewed last quarter as the bank ' s internal schedule required.

What should the KYC team manager do?

A. Submit a referral to file a suspicious activity report (SAR)

B. Evaluate the KYC review process to understand why the review did not occur as required and take corrective action as necessary

C. Contact the customer ' s relationship manager to suspend account access until the periodic KYC review is completed

D. Remove the customer from the bank ' s high-risk list

ANSWER: B

Explanation:

Evaluate the KYC review process to understand why the review did not occur as required and take corrective action as necessary is the appropriate response. A missed review of a high-risk relationship is a control failure requiring prompt remediation and root-cause analysis. The manager should ensure the overdue review is completed using the institution's risk-based customer due diligence procedures, determine whether the failure resulted from issues such as inadequate workflow controls, staffing, escalation, system configuration, or supervisory oversight, and implement proportionate corrective measures. Those measures may include revising tracking controls, addressing capacity gaps, retraining staff, improving exception reporting, and documenting management's resolution. High-risk customers require enhanced monitoring and more frequent review because their relationships present greater exposure to money-laundering or other financial-crime risk. A sound compliance program therefore needs controls that identify missed review deadlines and correct the underlying process weakness, rather than treating the missed deadline alone as evidence of suspicious activity. The Financial Crimes Enforcement Network's customer due diligence requirements emphasize ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information. The Federal Financial Institutions Examination Council likewise describes independent testing and oversight as key components for identifying and addressing Bank Secrecy Act/anti-money-laundering program weaknesses. See FinCEN's Customer Due Diligence Rule resources and the FFIEC BSA/AML Examination Manual.

QUESTION NO: 15

An existing customer at a bank has recently expanded its services to provide check cashing for its customers.

Which factor indicates the bank should terminate this relationship?

A. The bank has not updated its automated monitoring system.

B. The business has no previous experience with this service.

C. The business has not updated its anticipated activity with the bank.

D. The business is now a Money Service Business and has not registered with FinCEN.

ANSWER: D

Explanation:

The business is now a Money Service Business and has not registered with FinCEN is the factor that supports terminating the relationship, provided the business is subject to the registration requirement. A person that cashes checks as a business is generally an MSB when its check-cashing activity exceeds the applicable regulatory threshold. MSBs must comply with core Bank Secrecy Act obligations, including registration with FinCEN unless an exception applies, and must establish an effective written anti-money-laundering program. Registration is not merely an administrative formality: it helps establish that the customer is operating within the legal and supervisory framework applicable to money-transmission and other money-services activity.

When an existing customer materially changes its business by beginning check-cashing services, the bank must reassess the customer's risk profile and perform appropriate ongoing due diligence. If the customer cannot demonstrate required registration or a valid exemption, the bank faces heightened legal, regulatory, and financial-crime risk in continuing to provide services. In that circumstance, the customer's apparent noncompliance with a foundational MSB requirement presents a risk that may not be acceptably mitigated, making relationship termination appropriate. FinCEN's definition and registration materials describe the relevant MSB framework, while the FFIEC manual addresses risk-based due diligence and monitoring for MSB customers. See FinCEN's MSB definition guidance and the FFIEC BSA/AML Examination Manual.

QUESTION NO: 16

Which action does the Financial Action Task Force (FATF) recommend be taken against jurisdictions that have strategic deficiencies?

A. Conduct due diligence

B. Apply counter-measures

C. Add the jurisdiction to the United Nations' list of sanctioned jurisdictions

D. Create an action plan to address the deficiencies without the support of the FATF

ANSWER: B

Explanation:

Apply counter-measures is the correct answer. FATF identifies certain jurisdictions with serious, strategic deficiencies in their anti-money laundering, counter-terrorist financing, and counter-proliferation financing regimes. For jurisdictions subject to FATF's strongest public warning, described as a "call for action," FATF calls on its members and urges all jurisdictions to apply counter-measures that are proportionate to the risks arising from that jurisdiction. The purpose is to protect the international financial system from material financial-crime risks and to encourage the jurisdiction to address its deficiencies effectively. Depending on the risk and domestic legal framework, counter-measures may include enhanced external-audit requirements, increased supervisory examination and reporting requirements for financial groups, restrictions on establishing branches or subsidiaries, or limits on financial relationships and transactions. FATF's Recommendation 19 establishes the framework for countries to apply enhanced due diligence and, where FATF calls for it, counter-measures in relation to higher-risk countries. FATF publishes its current statements and lists through its high-risk and other monitored jurisdictions process; firms should use those publications alongside applicable national rules when calibrating country-risk controls. See FATF: High-risk and other monitored jurisdictions and FATF Recommendations.

QUESTION NO: 17

An internal audit team is reviewing the anti-financial crime (AFC) program of its firm.

Which of the following attributes of the third line of defense would be most critical to ensure unbiased and effective oversight?

A. Consistency of approach

B. Periodic training of the function

C. Qualification of the team

D. Independent testing

ANSWER: D

Explanation:

Independent testing is the most critical attribute because the third line of defense—internal audit—must be able to assess the design and operating effectiveness of the AFC program objectively. This includes evaluating governance, customer due diligence, transaction monitoring, sanctions controls, suspicious-activity reporting, escalation, and remediation without being responsible for operating those controls or being subject to inappropriate influence from the business or compliance functions. Independence enables internal audit to form evidence-based conclusions, report material issues candidly to senior management and the board or audit committee, and validate whether management has corrected identified deficiencies. The Institute of Internal Auditors' Three Lines Model identifies internal audit as providing independent and objective assurance, with accountability to the governing body. In an AML context, independent testing is also a core program expectation: testing should be performed by qualified personnel who are sufficiently independent of the function being reviewed. This organizational and functional separation is what makes audit oversight unbiased and credible, and it supports reliable challenge of both first-line execution and second-line compliance oversight. See the IIA Three Lines Model and the FFIEC BSA/AML examination guidance on independent testing.

QUESTION NO: 18

Which two channels can be utilized during a cross-border money laundering investigation to assist in gathering information according to Financial Action Task Force? (Choose two.)

A. Contacting existing liaison officers in the foreign jurisdiction

B. Exchanging information between national law enforcement agencies

C. Contacting the potential suspect or their family members to request information

D. Submitting only formal requests for information to a financial intelligence unit

ANSWER: A B

Explanation:

Contacting existing liaison officers in the foreign jurisdiction is an appropriate channel because liaison officers and attachés provide an established operational link between authorities. They can help investigators identify the appropriate foreign counterpart, clarify available information, coordinate urgent enquiries, and facilitate lawful informal cooperation before or alongside a formal request. This supports the Financial Action Task Force expectation that international cooperation be timely, constructive, and effective.

Exchanging information between national law enforcement agencies is also a core cross-border investigative channel. Direct agency-to-agency cooperation can enable the rapid sharing of intelligence, investigative leads, identities, locations, and other information needed to develop a money-laundering case. Financial Action Task Force standards call for competent authorities to have clear mechanisms for cooperation and information exchange with foreign counterparts, subject to domestic law, confidentiality controls, and appropriate restrictions on the use of information. Such cooperation is particularly valuable at the intelligence-development stage, when investigators need to map persons, assets, transactions, and related jurisdictions quickly.

These channels reflect the Financial Action Task Force emphasis on using both formal and appropriate informal international-cooperation mechanisms to support effective money-laundering investigations. See the Financial Action Task Force Recommendations and its best practices on international cooperation.

QUESTION NO: 19

How does the Financial Action Task Force (FATF) communicate its findings regarding jurisdictions with strategic anti-money laundering / Counter Financing of Terrorism deficiencies?

A. By issuing documentation to the private sector

B. By issuing two formal documents three times per year

C. By issuing informal communication to FATF members

D. By issuing four formal documents to the deficient jurisdictions

ANSWER: B

Explanation:

By issuing two formal documents three times per year is correct because FATF publicly communicates the results of its ongoing review of jurisdictions with strategic AML/CFT deficiencies through two principal statements issued after its Plenary meetings. “High-Risk Jurisdictions subject to a Call for Action” identifies jurisdictions with serious, strategic deficiencies for which FATF calls on members and the wider international community to apply enhanced due diligence and, in the most serious cases, countermeasures. “Jurisdictions under Increased Monitoring” identifies jurisdictions that have committed to resolving identified strategic deficiencies within agreed timeframes and are subject to enhanced follow-up. These publications are commonly described as the FATF black list and grey list, although FATF uses the formal titles. FATF Plenary meetings are generally held three times annually, so the statements are ordinarily reviewed and updated on that cycle. Publishing these documents provides transparent, consistent risk information that governments, supervisors, financial institutions, and designated non-financial businesses can incorporate into country-risk assessments, customer due diligence, correspondent-banking controls, and other AML/CFT risk-management measures. FATF’s official overview is available at FATF: High-risk and other monitored jurisdictions, and its current statements are published through the FATF publications page.

QUESTION NO: 20

The effectiveness of AML/CFT measures can be best measured by the extent to which systems and controls:

A. Comply with relevant laws and regulations

B. Minimize operational burden placed on the financial institution

C. Mitigate the risks and threats of financial crime

D. Are implemented in a cost-effective way

ANSWER: C

Explanation:

Mitigate the risks and threats of financial crime is correct because the fundamental purpose of an AML/CFT framework is to produce real-world outcomes that reduce money laundering, terrorist financing, and associated predicate-crime risks. Effective controls do more than exist on paper: they use a risk-based approach to identify relevant threats and vulnerabilities, apply proportionate preventive and detective measures, escalate meaningful concerns, and help prevent the financial system from being misused.

FATF assesses effectiveness through immediate outcomes, focusing on whether a jurisdiction’s and institution’s AML/CFT measures achieve their intended results in practice. This outcome-oriented approach recognizes that technical compliance with requirements is important, but it is not itself proof that controls are reducing financial-crime risk. A sound program should enable timely risk identification, appropriate customer due diligence and monitoring, useful suspicious-activity reporting, and support for competent authorities’ disruption of illicit finance.

This also reflects the risk-based principle: institutions must understand their exposure and allocate controls in a manner that manages and mitigates the identified risks. The central measure of success is therefore the extent to which the program meaningfully mitigates financial-crime threats, consistent with the FATF’s evaluation methodology and risk-based guidance. See the FATF assessment methodology and the FATF Recommendations.

QUESTION NO: 21

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

A. allows Financial Intelligence Units (FIUs) to enact sanctions against perpetrators of financial crime

B. promotes financial transparency and protects the integrity of the financial systems

C. needs to be approved by the Financial Intelligence Unit (FIU) before sharing between financial institutions

D. helps financial institutions to be more effective in fighting crime with data analysis

ANSWER: B

Explanation:

"promotes financial transparency and protects the integrity of the financial systems" is correct because timely, lawful exchange of relevant AML/CFT information enables institutions and competent authorities to develop a more complete picture of customer activity, beneficial ownership, transactions, and cross-border financial flows. That fuller picture supports the detection, assessment, and reporting of suspicious activity, while reducing the opportunity for criminals to exploit fragmented information across firms or jurisdictions. It also improves the quality of risk-based controls and supervisory oversight, which are central to preserving confidence in the financial system.

FATF standards expressly emphasize national and international cooperation and information exchange as essential elements of an effective AML/CFT regime. In particular, FATF Recommendation 2 requires domestic cooperation and coordination among relevant authorities, and the FATF methodology evaluates whether information can be shared effectively. The EU AML framework similarly requires cooperation and information exchange among financial intelligence units and other competent authorities. These frameworks treat appropriate data sharing—subject to confidentiality, privacy, and data-protection safeguards—as a means of increasing transparency and protecting the financial system from money laundering and terrorist-financing abuse. See FATF Recommendations and Directive (EU) 2015/849.

QUESTION NO: 22

Which factors specific to the securities industry increase the exposure to money laundering risk? (Select Two.)

A. The increase of sector-specific guidance

B. The practice of brokerage firms maintaining securities as nominees

C. The complexity of the securities business

D. The link to sanctioned countries

E. The speed of the transactions

ANSWER: B E

Explanation:

The practice of brokerage firms maintaining securities as nominees and the speed of the transactions are securities-industry characteristics that can heighten money-laundering exposure. Nominee or "street name" holdings may separate the registered holder from the underlying beneficial owner. Where intermediaries, omnibus accounts, or cross-border custody arrangements are involved, this structure can make it more difficult to establish who ultimately owns or controls an asset, understand the purpose of the relationship, and maintain a clear audit trail. Effective customer due diligence and beneficial-ownership procedures are therefore particularly important in this environment.

The speed of the transactions also creates risk because securities can be bought, sold, transferred, and liquidated rapidly, often across accounts, products, and markets. Criminals may seek to use that velocity to move value quickly, layer transactions, or exit positions before unusual activity is identified and investigated. Broker-dealer AML programs should consequently use surveillance, escalation procedures, and staffing that are calibrated to the firm's transaction volume and the rapidity of market activity. FINRA describes broker-dealers' AML-program obligations at FINRA's Anti-Money Laundering resource page; FATF provides sectoral risk material at FATF Methods and Trends.

QUESTION NO: 23

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

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

A. Whether the VASP's procedures are sufficient for protecting client personally identifiable information

B. What percentage of the VASP's clients are classified as higher-risk

C. Which registered institutions act on behalf of the VASP as operators of virtual asset wallets and virtual asset exchange offices

D. Whether the VASP is utilizing central bank digital currencies

E. Who the VASP's clients are, including the breakdown of foreign and domestic individuals

ANSWER: B C E

Explanation:

"What percentage of the VASP's clients are classified as higher-risk," "Which registered institutions act on behalf of the VASP as operators of virtual asset wallets and virtual asset exchange offices," and "Who the VASP's clients are, including the breakdown of foreign and domestic individuals" are material inputs to a financial institution's customer risk assessment. A VASP's underlying customer base can create indirect exposure for the institution, particularly where the VASP serves customers with elevated money-laundering, terrorist-financing, sanctions, or fraud risk. The proportion of such customers helps assess the scale of that exposure and whether the VASP's controls must be commensurately mature.

Understanding institutions that operate wallets or exchange services on the VASP's behalf identifies reliance on intermediaries and supports assessment of their registration, licensing, jurisdictions, and AML/CFT control environment. This is especially important because VASP services may be delivered through complex operational arrangements. Customer identity and domestic-versus-foreign composition are also central to evaluating customer and geographic risk, including cross-border exposure to jurisdictions with differing supervisory and AML/CFT standards. FATF's risk-based approach calls for assessment of customer, geographic, product/service, transaction, and delivery-channel risk factors, applied proportionately to the relationship. See the FATF Guidance for a Risk-Based Approach to Virtual Assets and VASPs and the FATF Recommendations.

QUESTION NO: 24

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

A. Fully rely on central beneficial owner registry records in the high-risk third country to determine the ultimate beneficial owners of all customers

B. Apply tailored due diligence measures, based on the level of risk posed by each customer following risk assessment

C. Monitor every cross-border transaction in real time, flagging all for enhanced scrutiny due to the country risk level

D. Automatically apply enhanced customer due diligence measures to all customers in the high-risk third-country branch regardless of risk level

ANSWER: B

Explanation:

Apply tailored due diligence measures, based on the level of risk posed by each customer following risk assessment is the most effective control because it operationalizes the risk-based approach at the customer level. A bank should identify and assess relevant customer, product, service, transaction, delivery-channel, and geographic risk factors, then calibrate customer due diligence, ongoing monitoring, and review frequency to the resulting risk profile. The branch's presence in a high-risk third country is an important geographic factor that should inform the bank-wide and branch-level risk assessment, governance, escalation, and monitoring arrangements. It does not remove the need to assess each relationship individually. A proportionate framework enables the bank to focus enhanced measures and investigative resources on relationships and activity that present higher money-laundering or terrorist-financing exposure, while still maintaining effective baseline controls for all customers. This approach also requires documented risk assessments, clear policies, sufficient management information, and periodic reassessment when customer circumstances or risk indicators change. EU AML rules require obliged entities to apply customer due diligence on a risk-sensitive basis, and the EBA guidance explains how firms should assess ML/TF risks and apply proportionate controls. See Directive (EU) 2015/849 and the EBA ML/TF Risk Factors Guidelines.

QUESTION NO: 25

The branch manager notices that a number of customers come in weekly and always use the same teller to process their deposits. The manager notices that the customers and the teller, who are from the same ethnic group, are speaking in a foreign language and every once in a while the customers from local ethnic restaurants will bring the teller lunch. The commercial customers that visit the teller generally deposit the same amount of cash each time they come in.

How should the branch manager respond to this activity?

A. Transfer the teller to another branch

B. Conduct further investigation before taking any other action

C. Encourage the teller to bring in more business from the ethnic community

D. Suggest to the teller to send the customers to other tellers to avoid the opportunity for collusion

ANSWER: B

Explanation:

Conduct further investigation before taking any other action is the appropriate response because the manager has observed a pattern that merits objective, risk-based review, rather than an immediate conclusion about either the teller or the customers. Customers' ethnicity, language, preference for a particular teller, and occasional customary hospitality do not themselves establish suspicious activity. However, recurring cash deposits by commercial customers in consistent amounts may warrant examination in the context of each business's expected cash activity, transaction history, source of funds, and any relationship among the customers or employee. The manager should follow internal BSA/AML escalation procedures, document relevant observations, and refer the matter to the appropriate compliance, investigations, or security personnel. A proper review can determine whether there is a reasonable explanation consistent with the customers' businesses or whether additional facts support suspicion of structuring, employee collusion, or another reportable concern. This approach supports fair treatment, avoids decisions based on protected characteristics, preserves confidentiality, and enables the institution to meet its obligation to identify, investigate, and, when appropriate, report suspicious activity. The FFIEC explains that suspicious-activity monitoring should identify unusual activity, assess it in relation to expected account behavior, and support appropriate investigation and SAR decisions. See the FFIEC BSA/AML Manual: Suspicious Activity Reporting and FinCEN's SAR reporting guidance.

QUESTION NO: 26

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:

Targeted sanctions, sectoral sanctions, and comprehensive sanctions are established categories of economic sanctions that financial institutions must distinguish when designing sanctions-compliance controls. Targeted sanctions—also called list-based or "smart" sanctions—apply to identified persons, entities, vessels, aircraft, or other designated parties. They commonly require asset-freeze measures and prohibit transactions or the provision of funds, goods, or services involving the designated target. Sectoral sanctions apply narrower restrictions to specified economic sectors or activities, such as defined financing, debt, equity, technology, or services involving energy, defense, or financial-services industries. Their application depends on transaction details and the parties' sectoral connections. Comprehensive sanctions broadly prohibit or severely restrict dealings involving an entire country or region, generally subject to stated exemptions, general licenses, or specific authorizations. These categories create distinct compliance requirements: effective name screening and ownership analysis for targeted restrictions, transaction and product controls for sectoral restrictions, and jurisdictional controls for comprehensive programs. OFAC explains that its programs may be country-based or list-based and may involve broad or selective restrictions; its current programs are available at [OFAC Sanctions Programs and Country Information]. A useful overview of the policy tools and forms economic sanctions may take is provided by the [Council on Foreign Relations].

QUESTION NO: 27

Which two mechanisms should be implemented to assist with cross-border money laundering investigations? (Choose two.)

A. Countries should request Interpol to provide the required information.

B. Countries should ensure that information received is protected from unauthorized disclosure.

C. Countries should establish mechanisms allowing financial investigators to obtain and share information in respect of specific investigations.

D. Countries should conduct separate investigations to ensure information is not unintentionally disclosed without the appropriate legal approval.

ANSWER: B C

Explanation:

Countries should ensure that information received is protected from unauthorized disclosure because international anti-money laundering cooperation depends on trust, confidentiality, and controls over the use of sensitive intelligence and evidentiary material. Information obtained through foreign counterparts may be subject to conditions governing its use, onward dissemination, storage, and disclosure in legal proceedings. Robust confidentiality safeguards allow financial intelligence units, law-enforcement agencies, supervisors, and other competent authorities to exchange information without compromising investigations, sources, or personal data.

Countries should establish mechanisms allowing financial investigators to obtain and share information in respect of specific investigations because effective cross-border cases require timely access to financial records, beneficial-ownership information, intelligence, and evidence held in another jurisdiction. Practical cooperation mechanisms can include mutual legal assistance, FIU-to-FIU information exchange, police-to-police cooperation, and other competent-authority channels. These arrangements support tracing assets, identifying transaction flows and associated parties, obtaining evidence, and pursuing freezing, seizure, confiscation, or prosecution actions. FATF Recommendation 40 requires countries to provide the widest possible range of international cooperation and to maintain clear, secure processes for exchanging information. See the [FATF Recommendations] and FATF's [best practices on information exchange].

QUESTION NO: 28

Which key factor would result in the decision for a financial institution (FI) to exit a client relationship?

A. After assessing all risk factors the level of residual client risk exceeds the FI's risk appetite.

B. The client is a registered charity known to remit funds to high risk geographies where there is limited due diligence information available.

C. Closing the client accounts will help reduce the number of transaction monitoring alerts.

D. Client transactions generate ongoing transaction monitoring alerts that did not result in any SAR/STR filings.

ANSWER: A

Explanation:

After assessing all risk factors, the level of residual client risk exceeds the FI's risk appetite is the key factor supporting an exit decision. A risk-based AML program requires an FI to identify the customer's inherent risk, conduct customer due diligence proportionate to that risk, and apply controls such as enhanced due diligence, transaction monitoring, restrictions, and senior-management oversight. Residual risk is the risk remaining after those measures have been applied. Where that remaining exposure is beyond the level the FI has formally determined it can accept and manage, continuing the relationship would be inconsistent with its risk-appetite framework and governance obligations. The appropriate outcome can therefore be an orderly refusal, restriction, or termination of the relationship, based on documented analysis and applicable legal, regulatory, contractual, and reporting requirements. FATF explains that risk-based measures should be commensurate with identified risks and emphasizes that institutions should assess and manage risk rather than apply indiscriminate approaches. U.S. supervisory guidance similarly frames customer-risk management around assessing risk and maintaining controls appropriate to the institution's risk profile. See the FATF Recommendations and the FFIEC BSA/AML Examination Manual.

QUESTION NO: 29

A division anti-money laundering officer for a financial institution has been conducting a monthly self-assessment.

The officer reviews the accounts opened for compliance with a long standing Know Your Customer policy.

The self-assessment for the latest month shows a significant increase in compliance deficiencies for the first time in more than a year.

Which of the following is the next course of action for the anti-money laundering officer to take?

A. Inform the Board promptly of the Know Your Customer policy trend over the last 6 months.

B. Determine if there is a readily identifiable cause for the deficiencies.

C. Implement a revision to the account-opening training program.

D. Revise the policy to simplify Know Your Customer compliance before the report is issued.

ANSWER: B

Explanation:

Determine if there is a readily identifiable cause for the deficiencies. A single-month, material rise in account-opening compliance deficiencies is an exception that requires prompt investigation before selecting or implementing remediation. The anti-money laundering officer should validate the assessment results and perform a focused root-cause analysis, considering whether a change in staffing, procedures, systems, products, customer volume, training, quality-assurance testing, or policy interpretation contributed to the trend. The inquiry should be sufficiently documented to establish the scope, severity, affected accounts, and any immediate customer or regulatory risk. Identifying the cause enables management to apply proportionate corrective action, such as targeted retraining, procedural clarification, system remediation, enhanced review of affected files, or escalation under the institution's governance process. This approach supports a risk-based compliance program: controls and remediation should be driven by verified weaknesses and their underlying causes rather than assumptions. U.S. regulatory guidance emphasizes that an effective anti-money laundering program includes internal controls, independent testing, and appropriate management of identified control weaknesses. See the FFIEC BSA/AML Manual and FinCEN's AML program requirements guidance.

QUESTION NO: 30

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:

“When new products, services or customer types are introduced” is correct because an FI’s ML/TF risk assessment must reflect its current inherent-risk profile. New offerings, delivery methods, or customer segments may introduce different transaction patterns, levels of customer anonymity, jurisdictions, payment mechanisms, or typologies. The FI should therefore assess the new exposure before launch or promptly when the change occurs, and ensure that customer due diligence, transaction monitoring, screening, governance, and staffing controls remain appropriate.

“When the institution faces a merger or acquisition” is also correct because a transaction of this nature can materially change the institution’s risk profile and control environment. The combined organization may acquire customers, products, geographies, agents, payment flows, data systems, and inherited control deficiencies that were not contemplated in the prior assessment. A refreshed assessment supports risk-based integration planning, including remediation priorities and calibration of AML controls. FATF Recommendation 1 requires institutions to identify, assess, and understand their ML/TF risks and apply measures proportionate to those risks; this necessarily includes keeping assessments current as material circumstances evolve. See FATF Recommendations and the FFIEC BSA/AML risk-assessment guidance.

QUESTION NO: 31

Whichsuspicious activitymay be thestrongest indicator of money laundering through a casino?

A. A privately held company originates funds transfers through the casino into the betting accounts of multiple patrons.

B. A patron routinely places multiple bets on the same sporting events.

C. A patron purchases a large amount of chips at a blackjack table using cash.

D. A patron requests the casino to transfer their winnings to another gambling operator.

ANSWER: A

Explanation:

A privately held company originates funds transfers through the casino into the betting accounts of multiple patrons is the strongest indicator because it combines third-party funding, the use of multiple apparently unrelated customer accounts, and an unclear commercial purpose. This activity can obscure the true source, ownership, and control of funds by placing company money into patron accounts, potentially using those patrons as nominees or money mules. The casino may then be used to convert the funds into gambling balances, chips, withdrawals, or purported winnings, creating a transactional record that can make illicit proceeds appear to have a legitimate gambling-related origin. Casinos should understand the source of funds and source of wealth where risk warrants it, identify beneficial ownership and relationships among parties, and investigate patterns that lack an apparent lawful purpose. Financial institutions and casinos are expected to monitor for unusual activity and file a suspicious activity report when they know, suspect, or have reason to suspect that a transaction involves illicit funds, is designed to evade reporting requirements, or lacks a lawful purpose. FATF identifies casinos as a sector subject to customer due diligence and suspicious-transaction reporting obligations. See FATF Recommendations and FinCEN casino guidance and resources.

QUESTION NO: 32

It is essential to identify any "family members" or "close associates" of politically exposed persons (PEPs) as part of the KYC/CDD process because they could be:

A. executing cross-border transactions for their own business which is not commensurate to the PEP's wealth.

B. in a position to provide more information regarding the PEP's whereabouts and hidden properties.

C. travelling to offshore jurisdictions often on holiday which exposes them to higher risks for AML.

D. used as intermediaries to facilitate bribery or corruption or to conceal the illicit wealth of the PEP.

ANSWER: D

Explanation:

Family members and close associates of a politically exposed person must be identified because they may be used as intermediaries to facilitate bribery or corruption or to conceal the illicit wealth of the PEP. A person entrusted with a prominent public function may have access to public funds, influence over government decisions, or exposure to bribery and embezzlement risks. Rather than placing assets or conducting transactions in their own name, that person may use relatives, business partners, nominees, or other close associates to hold beneficial ownership interests, move funds, receive corrupt payments, or obscure the source and destination of assets. Identifying these connected persons enables an institution to establish beneficial ownership, understand the purpose and expected activity of the relationship, assess the PEP-related risk, and apply appropriate enhanced due diligence and ongoing monitoring. The Financial Action Task Force specifically requires financial institutions to take reasonable measures to identify family members and close associates of foreign PEPs, recognizing that these relationships can provide channels through which PEP-linked illicit proceeds are concealed or transferred. This approach supports effective detection of corruption proceeds while using a risk-based assessment rather than treating every connected person as automatically involved in wrongdoing. See the FATF Recommendations and FATF's guidance on politically exposed persons.

QUESTION NO: 33

When the Financial Action Task Force (FATF) places a jurisdiction on the list of "jurisdictions under increased monitoring," also known as the "grey list," the jurisdiction:

A. Accepts to participate in an off-cycle FATF mutual evaluation to be held within the next 12 months.

B. Must pay a fine to be removed from the list before the next FATF plenary.

C. Has committed to swiftly resolving the deficiencies identified in a FATF mutual evaluation.

D. Poses a high money laundering, terrorist financing and proliferation financing risk and must be restricted from accessing the international financial system.

ANSWER: C

Explanation:

Has committed to swiftly resolving the deficiencies identified in a FATF mutual evaluation. FATF places a jurisdiction under increased monitoring when it is actively working with FATF to address strategic deficiencies in its anti-money laundering, counter-terrorist financing, and counter-proliferation financing framework within agreed timeframes. A jurisdiction included in this process has made a high-level political commitment to implement an action plan designed to remedy the weaknesses identified through its mutual evaluation and subsequent FATF review.

Inclusion on the grey list is therefore a monitoring and remediation mechanism, not a punitive fine or an automatic exclusion from the international financial system. FATF's public statements identify the jurisdiction, summarize its strategic deficiencies, and describe the actions expected for removal from increased monitoring. Financial institutions should use a risk-based approach and consider the relevant FATF information in their country-risk assessments and controls. FATF also states that its listing does not, by itself, require enhanced due diligence measures; such measures remain subject to each institution's risk assessment and applicable legal requirements. See FATF's High-Risk and Other Monitored Jurisdictions page and its Methodology for Assessing Technical Compliance and Effectiveness.

QUESTION NO: 34

Which methods are typically used to launder money using insurance companies? (Choose two.)

A. The policy holder overpays the policy and moves the funds out of the policy despite paying early withdrawal penalties.

B. The policy holder enters a sibling as a beneficiary of the insurance policy rather than themselves.

C. The policy holder purchases a bond and redeems it at a discount prior to its full term.

D. The policy holder uses an offshore company to pay the insurance installments.

E. The policy holder is strongly interested in how many costs are incurred when taking out an insurance policy.

ANSWER: A D

Explanation:

The policy holder overpays the policy and moves the funds out of the policy despite paying early withdrawal penalties is a recognized insurance-sector laundering typology. An individual can place illicit funds into a cash-value or investment-linked policy through unusually large premium payments, then surrender the policy or obtain a withdrawal or refund. Accepting a financial penalty may be commercially irrational for a legitimate customer, but it can be worthwhile to a launderer because the returned funds originate from an established insurer and may appear more legitimate. The policy holder uses an offshore company to pay the insurance installments is also a material laundering method and red flag. A corporate third-party payer, particularly one located offshore, can obscure the actual source of funds, the relationship between the payer and insured, and beneficial ownership. It may additionally introduce cross-border layering and make verification of the underlying business purpose more difficult. Insurance AML programs should therefore assess source of funds and wealth, verify the rationale for third-party premium payments, identify beneficial owners, and scrutinize unusual overpayments, early surrenders, and refunds. These typologies are described in the FATF's insurance-sector money-laundering research and are consistent with insurance AML supervisory guidance. See FATF: Money laundering and terrorist financing through insurance and the NAIC Insurance Anti-Money Laundering Guidance Manual.

QUESTION NO: 35

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

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

A. Opening an account to settle an estate on behalf of a client

B. Establishing shell companies to enable money laundering activities, including placement or layering

C. Opening third-party accounts for the primary purpose of masking the underlying client's identity

D. Opening a trust account to facilitate a legitimate real estate transaction

E. Directing or facilitating the laundering of illicit funds, including structuring transactions

ANSWER: B C E

Explanation:

Establishing shell companies to enable money laundering activities, including placement or layering, is a significant financial-crime risk because legal persons can be used to conceal the identity of beneficial owners, distance criminals from illicit assets, and create a seemingly legitimate structure for moving value. Opening third-party accounts for the primary purpose of masking the underlying client's identity is likewise high risk: it obscures who controls funds and prevents the institution from applying effective customer due diligence, beneficial-ownership verification, and transaction monitoring to the true party. Directing or facilitating the laundering of illicit funds, including structuring transactions, reflects direct professional involvement in disguising the source, ownership, or movement of criminal proceeds. Structuring can be used to evade reporting or detection thresholds, while professional expertise may lend transactions an appearance of legitimacy. These risks align with the Financial Action Task Force's focus on transparency of legal persons and customer due diligence for designated non-financial businesses and professions. See the FATF Recommendations, particularly the standards addressing customer due diligence, beneficial ownership, and professional intermediaries, and FATF's guidance on beneficial ownership transparency.

QUESTION NO: 36

What areas of laws and regulations have the greatest impact on AML/CFT applications? (Choose three.)

A. Information security, data privacy, and cybersecurity

B. Foreign exchange control, and precious gemstone and metal dealing

C. Ombudsman and anti-competition authority

D. Electronic contract and biological signature acceptance

E. Consumer protection, financial inclusion, and environmental, social and governance

ANSWER: A B E

Explanation:

Information security, data privacy, and cybersecurity; **Foreign exchange control, and precious gemstone and metal dealing**; and **Consumer protection, financial inclusion, and environmental, social and governance** are the areas with the broadest practical impact on AML/CFT applications. AML/CFT systems collect, retain, screen, analyze, and sometimes share highly sensitive customer and transaction information. Information-security, privacy, and cybersecurity requirements therefore directly shape system access controls, data governance, retention, security monitoring, and incident management. The FATF Recommendations recognize that effective AML/CFT measures must be implemented consistently with data-protection and privacy requirements.

Foreign-exchange activity and dealings in precious metals or stones are important AML/CFT risk areas because they can involve cross-border value movement, high-value transactions, and nonfinancial businesses subject to risk-based controls. These requirements affect customer due diligence, recordkeeping, transaction monitoring, and suspicious-transaction reporting workflows. Consumer-protection and financial-inclusion obligations also influence how firms implement risk-based controls without unnecessarily excluding legitimate customers. Environmental, social and governance considerations increasingly inform financial-crime risk assessments, particularly where environmental crime, corruption, or supply-chain risks can generate illicit proceeds. FATF's risk-based framework supports proportionate controls that address these intersecting legal and regulatory demands. See the FATF Recommendations and FATF's financial inclusion resources.

QUESTION NO: 37

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

A. collaborating with law enforcement agencies, financial institutions, and other stakeholders to detect and prevent Illicit financial activities.

B. conducting examinations of financial institutions to ensure compliance with anti-money laundering regulations.

C. engaging in providing financial services, including banking and investment activities, to the public and private sectors

D. facilitating the exchange of information between the public and private sectors.

E. enacting legislation regarding the operations of financial institutions.

ANSWER: A D

Explanation:

"collaborating with law enforcement agencies, financial institutions, and other stakeholders to detect and prevent Illicit financial activities" is correct because an FIU is the national centre for receiving, analysing, and disseminating financial-intelligence information related to suspected money laundering, associated predicate offences, and terrorist financing. Effective performance of those functions requires operational cooperation with reporting institutions, law-enforcement authorities, supervisors, and, where appropriate, foreign FIUs. This collaboration helps convert suspicious transaction reports and other relevant data into actionable intelligence for competent authorities.

"facilitating the exchange of information between the public and private sectors" is also correct. FIUs commonly support information sharing by issuing typologies, red-flag indicators, strategic analysis, and feedback to reporting entities, while receiving reports and other relevant information from the private sector. Such two-way engagement improves reporting quality, strengthens detection capabilities, and supports a coordinated national AML/CFT framework. FATF Recommendation 29 establishes the FIU's central role in receiving, analysing, and disseminating financial intelligence, and the Egmont Group describes FIUs' role in exchanging financial intelligence domestically and internationally. See FATF Recommendations and Egmont Group—Financial Intelligence Units.

QUESTION NO: 38

A law enforcement agency is reviewing a suspicious transaction report (STR) filed by a financial institution for suspicious activity on a client's account.

Subsequently, the agency requests further information.

Which supporting documentation might the law enforcement agency request from the institution to facilitate its investigation?

A. Previously filed STRs on the same customer

B. Account opening documents and account statements

C. Copies of promotional materials sent to the customer

D. A copy of the institution's STR policy and procedures

ANSWER: B

Explanation:

Account opening documents and account statements are the most useful supporting records for a law enforcement investigation following an STR. Account-opening records establish the customer's identity, the nature and purpose of the relationship, beneficial-ownership information where applicable, and information the customer supplied concerning expected account activity or source of funds. Statements and underlying transaction records then provide the chronological evidence needed to assess the suspicious activity: amounts, dates, payment instructions, counterparties, cash activity, wire-transfer details, and patterns that may connect the account to other persons or entities.

These business records enable investigators to corroborate the facts summarized in the STR, trace the movement of funds, identify associated accounts and counterparties, and develop appropriate legal process or investigative leads. Financial institutions should retain records supporting their suspicious-activity reporting and make responsive underlying documents available to authorized authorities through the applicable information-sharing or legal-process channels. The STR itself is intended to provide a concise narrative and key data; the customer and transaction documentation supplies the evidentiary detail needed to advance the investigation. FinCEN emphasizes the value of complete supporting documentation and transaction data in suspicious-activity reporting and follow-up investigations. See FinCEN SAR Activity Review and FinCEN SAR Trends, Tips & Issues.

QUESTION NO: 39

Which ML/TF risks are associated with cryptoassets? (Select Three.)

A. Devaluation

B. Smart contract vulnerabilities

C. Potential for anonymity

D. Global reach

E. High transaction fees

F. Use to layer illicit funds

ANSWER: C D F

Explanation:

"Potential for anonymity," "Global reach," and "Use to layer illicit funds" are core ML/TF risks associated with cryptoassets. Cryptoasset transfers may be conducted using wallet addresses rather than directly visible real-world identities. Although many blockchain transactions are publicly recorded and can be analyzed, anonymity-enhancing features, unhosted wallets, weak customer due diligence, and the use of intermediaries in poorly regulated jurisdictions can make it difficult to identify the persons controlling funds. Cryptoassets also permit fast, borderless value transfers, allowing criminals or terrorist financiers to move assets across jurisdictions outside traditional correspondent-banking channels and exploit uneven international regulatory and supervisory coverage. In addition, the ability to transfer value rapidly among multiple wallet addresses, virtual asset service providers, exchanges, chains, or conversion services can support layering intended to obscure the origin, ownership, and trail of illicit proceeds. These characteristics require a risk-based AML/CFT approach, including customer due diligence, transaction monitoring, sanctions screening, suspicious activity reporting, and attention to blockchain-related typologies and red flags. FATF identifies anonymity, cross-border reach, and the capacity to move or obscure illicit value among the principal ML/TF risk factors relevant to virtual assets and virtual asset service providers. See FATF's guidance on virtual assets and VASPs and FATF virtual-asset red-flag indicators.

QUESTION NO: 40

The United Nations Security Council (UNSC) is empowered to impose sanctions regimes against countries and terrorist organizations.

Which statements are true regarding sanctions imposed by the UNSC? (Select Two.)

A. Attempts to circumvent or evade sanctions imposed by the UNSC can constitute a criminal offense if designated under local laws and regulations

B. The UN can impose arms embargoes but cannot prohibit direct or indirect exports of other goods to specific countries

C. Member countries of the United Nations are expected to implement and enforce sanctions imposed by the UNSC

D. Direct breaches of sanctions imposed by the UNSC constitute a criminal offense in all member countries

ANSWER: A C

Explanation:

"Attempts to circumvent or evade sanctions imposed by the UNSC can constitute a criminal offense if designated under local laws and regulations" is correct because Security Council sanctions are implemented through each UN Member State's domestic legal and regulatory framework. Although the Security Council establishes the measures, national authorities give them legal effect, supervise compliance, investigate suspected evasion, and determine the applicable civil or criminal penalties. Consequently, attempted evasion—such as concealing the sanctioned party's involvement, falsifying trade documentation, or structuring a transaction to avoid an asset freeze—may be criminalized where domestic implementing legislation so provides.

"Member countries of the United Nations are expected to implement and enforce sanctions imposed by the UNSC" is also correct. Under Article 25 of the UN Charter, UN Members agree to accept and carry out Security Council decisions. When the Council adopts binding measures under Chapter VII, Member States must take appropriate action to implement those measures, including asset freezes, travel restrictions, arms embargoes, and targeted trade or financial restrictions. Effective implementation requires regulated institutions to screen relevant parties and transactions, freeze assets or reject prohibited activity where required, and report as required by the applicable national regime. See the UN Charter and the UN Security Council's sanctions information page.

QUESTION NO: 41

A foreign politically exposed person (PEP) requests to add a beneficiary to a life insurance policy.

How should the request be processed to mitigate risk?

A. Perform due diligence on the beneficiary

B. Determine the source of wealth and source of funds

C. Decline the request if the beneficiary is a foreign PEP

D. Decline the request to add a beneficiary due to increased risk

ANSWER: A

Explanation:

Perform due diligence on the beneficiary is the appropriate risk-mitigation step because adding a beneficiary changes the person who may ultimately receive the policy proceeds. Life-insurance products can be misused to transfer value to an undisclosed or inappropriate recipient, and the beneficiary is therefore a relevant party in assessing the risk of the requested change. The insurer should obtain and assess sufficient information to understand the beneficiary's identity, relationship to the policyholder, and the plausibility of the designation in light of the customer's profile and the policy's purpose. Risk-based screening and review should identify relevant sanctions exposure, PEP status, and credible adverse information, with the review and approval documented under the insurer's AML procedures. This beneficiary-focused review is particularly important where the policyholder is a foreign PEP, since the relationship presents elevated corruption and misuse-of-office risk. FATF's customer due-diligence framework requires financial institutions to identify and assess beneficial interests and apply enhanced measures when risk is higher. FATF's life-insurance sector guidance specifically recognizes beneficiaries as important parties for AML/CFT controls and risk assessment. See the FATF Recommendations and FATF's risk-based approach guidance for the life-insurance sector.

QUESTION NO: 42

What is the primary purpose of anti-bribery and corruption regulations?

A. To prohibit the payment of anything of value by persons or entities to government officials or employees of state-owned enterprises to obtain an improper business advantage

B. To prohibit the conversion of illegally obtained money into legal money by senior government figures

C. To protect against election interference by corrupt foreign adversaries facilitated by illicit funds

D. To protect against the use of illegal means by senior political figures to avoid paying taxes

ANSWER: A

Explanation:

The primary purpose of anti-bribery and corruption regulations is to prevent persons and entities from offering, promising, authorizing, or paying anything of value to government officials—including employees of state-owned enterprises—when the intent is to obtain or retain business or secure an improper business advantage. This is a core anti-corruption principle reflected in major legal frameworks used in financial-crime compliance programs. For example, the U.S. Foreign Corrupt Practices Act addresses corrupt payments to foreign officials for the purpose of obtaining or retaining business, while the UK Bribery Act similarly criminalizes bribery intended to induce improper performance or obtain an advantage. In practice, these rules require organizations to implement risk-based controls such as due diligence on third parties, approval processes for gifts, travel, and hospitality, accurate books and records, training, and escalation of suspicious conduct. The focus is not merely on the transfer of money; "anything of value" can include gifts, travel, charitable donations, employment opportunities, or other benefits when offered corruptly. This objective helps protect fair competition, public integrity, and the legitimacy of commercial and governmental decision-making. See the U.S. Department of Justice's FCPA resource and the UK Bribery Act 2010.

QUESTION NO: 43

A large international financial institution (FI) operates in both the United States and the European Union. A cross-border transaction involving a high-net-worth client with dual U.S. and French citizenship raises concerns due to a third-party intermediary in a high-risk jurisdiction.

Given that the transaction falls under the U.S. Bank Secrecy Act (BSA) and OFAC requirements, as well as the EU's 6th Anti-Money Laundering Directive (6AMLD) and European Banking Authority (EBA) regulations, what is the best approach for the compliance team to ensure compliance?

A. Follow EU regulations only, as the beneficiary is based in France

B. Implement a dual-compliance approach satisfying both U.S. and EU AFC regulations

C. Defer to the most stringent regulatory regime to streamline compliance

D. Follow U.S. regulations only, as the transaction originates in the United States

ANSWER: B

Explanation:

Implement a dual-compliance approach satisfying both U.S. and EU AFC regulations is correct because the facts establish regulatory touchpoints in both jurisdictions. The institution should apply a coordinated, risk-based process that meets the applicable U.S. Bank Secrecy Act requirements—including customer due diligence, transaction monitoring, recordkeeping, and suspicious activity reporting—and its OFAC obligations to screen relevant parties and assess any sanctions nexus. FinCEN explains that the BSA framework requires financial institutions to help detect and report suspected money laundering and other financial crime through their AML programs and reporting obligations. See FinCEN's Bank Secrecy Act resources.

At the same time, the EU connection requires the institution to follow applicable EU and member-state AML/CFT requirements, including risk-sensitive due diligence and enhanced measures where the customer, intermediary, or transaction presents higher risk. The EBA's AML/CFT guidance emphasizes effective policies, controls, governance, and a risk-based approach across the institution. A single integrated case assessment can avoid duplication, but it must preserve each jurisdiction's distinct reporting routes, deadlines, screening standards, documentation, and escalation requirements. This approach is especially important when a third-party intermediary is linked to a high-risk jurisdiction. See the EBA AML/CFT regulatory resources.

QUESTION NO: 44

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

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

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

B. The assets acquired through an auction were put in the name of an offshore company

C. The agent acted on behalf of an individual residing in a country which is on the EU's list of high-risk jurisdictions

D. The power of attorney was issued by a law firm in a different EU country from where the transaction took place.

ANSWER: A C

Explanation:

The agent requested a disposal of assets at a lower price than recently acquired is a significant transaction red flag. A rapid resale at a substantial discount from a recent, objectively documented auction price may indicate an attempt to transfer value covertly, conceal the beneficial economic purpose of the transaction, or distance assets from their source. The notary should understand the commercial rationale for the price, assess whether the declared consideration is credible, and consider whether the urgency and refusal to discuss the discrepancy heighten suspicion. Such facts can support enhanced scrutiny and, where the applicable legal threshold is met, consideration of a suspicious-transaction report.

The agent acted on behalf of an individual residing in a country which is on the EU's list of high-risk jurisdictions also requires heightened attention. The European Union identifies high-risk third countries with strategic anti-money-laundering and counter-terrorist-financing deficiencies. Transactions connected to those jurisdictions are subject to enhanced customer due diligence under the EU framework, including obtaining additional information and increased monitoring appropriate to the risk. The notary should therefore establish the parties, beneficial ownership, source of funds and wealth, and the purpose of the proposed disposal. See the European Commission's high-risk third-country information and Directive (EU) 2015/849.

QUESTION NO: 45

What key element contributes to the effectiveness of AML training programs'?

A. In-person training sessions

B. Comprehensive curriculum delivered by senior management

C. Comprehensive content with engaging delivery methods

D. Generalized content designed to apply to a broad audience

ANSWER: C

Explanation:

Comprehensive content with engaging delivery methods is the key element because effective AML training must both provide employees with the knowledge needed for their specific anti-money laundering responsibilities and present that knowledge in a way that supports attention, understanding, and practical application. A sound curriculum covers relevant legal and regulatory obligations, internal policies and procedures, customer due diligence, suspicious activity identification and escalation, and the consequences of noncompliance. Its content should be tailored to the institution's products, services, customer risks, and the employee's role.

Engaging delivery methods—such as realistic scenarios, case studies, interactive discussions, short assessments, and role-specific examples—help staff recognize red flags and make appropriate decisions in real working situations. This makes training more likely to change behavior rather than merely document attendance. Training should also be delivered regularly and updated as risks, typologies, products, systems, or regulatory expectations change. U.S. supervisory guidance describes an effective training program as one tailored to particular responsibilities and inclusive of periodic training on the BSA/AML program and relevant requirements. See the FFIEC BSA/AML Examination Manual and FinCEN's statutes and regulations resources.

QUESTION NO: 46

Which are red flags indicating potential engagement of a bank employee in money laundering? (Select Two.)

A. Lavish lifestyle that cannot be supported by an employee's salary

B. Reluctance to take a vacation when the employee has sufficient leave

C. Failure to meet business goals for more than one period

D. Providing longer than usual services for a certain customer

E. Maintaining friendships with customers and going to restaurants, games, and other events

ANSWER: A B

Explanation:

"Lavish lifestyle that cannot be supported by an employee's salary" is a significant insider-risk red flag. An unexplained increase in wealth, expensive purchases, or spending inconsistent with known compensation can indicate that an employee is receiving bribes, kickbacks, or a share of illicit proceeds in return for facilitating transactions, onboarding customers improperly, overriding controls, or disclosing confidential information. Institutions should have proportionate employee-monitoring and escalation processes that enable concerns of this type to be assessed appropriately.

"Reluctance to take a vacation when the employee has sufficient leave" is also a recognized warning sign of potential internal misconduct. An employee involved in concealing improper activity may seek to remain continuously in control of accounts, records, approvals, or customer relationships so that irregularities are not discovered by a substitute. Mandatory consecutive leave, job rotation, independent review, and segregation of duties are therefore valuable controls: they can expose hidden transactions, unauthorized account activity, and control circumvention when another person performs the employee's work. The FFIEC emphasizes that a BSA/AML program requires internal controls designed to assure ongoing compliance, while FinCEN's AML program materials describe the central role of internal controls in detecting and reporting suspicious activity. See the FFIEC BSA/AML Examination Manual and FinCEN AML Act resources.

QUESTION NO: 47

What are two reasons physical certificates present a money laundering risk to broker-dealers? (Choose two.)

A. The trade information on a physical certificate can be easily altered

B. Physical certificates do not expire and may be held by the owner for perpetuity

C. There is little information readily available to the broker confirming the source of the funds

D. Physical certificates may be provided to nominees for deposit or settled in off-market transactions

ANSWER: C D

Explanation:

Physical certificates can create an AML vulnerability because the broker-dealer may have little readily available information that confirms the source of funds or wealth represented by the security. Unlike positions acquired and maintained through an account with an established electronic trading and settlement record, a paper certificate may be presented for deposit with limited information about its acquisition, prior ownership, or intervening transfers. This limits the firm's ability to assess whether the asset is consistent with the customer's known profile and expected activity, and supports the need for risk-based due diligence and investigation of suspicious activity.

Physical certificates also may be provided to nominees for deposit or settled in off-market transactions. A nominee can obscure the identity of the person who beneficially owns or controls the security, while off-market transfers can reduce the transparency normally supplied by centralized clearing, custody, and book-entry systems. These features may help a criminal move or liquidate value while complicating the audit trail and the broker-dealer's ability to identify linked parties and suspicious patterns. Broker-dealers should apply their AML program, customer identification, and suspicious-activity monitoring obligations to activity involving securities certificates. See the SEC's discussion of holding securities and book-entry ownership and FinCEN's AML guidance and resources.

QUESTION NO: 48

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:

"Demonstrate a high-level commitment to swiftly resolve the identified deficiencies in the FATF mutual evaluation report." is correct because FATF's International Co-operation Review Group process requires a jurisdiction with strategic deficiencies to make a high-level political commitment to address them. That commitment is ordinarily formalized through an agreed action plan identifying the reforms, responsible authorities, and target timeframes needed to strengthen the country's AML/CFT/CPF framework. FATF's public materials on jurisdictions under increased monitoring emphasize that political commitment and timely action-plan implementation are core elements of the monitoring process.

"Report to FATF on the implementation of their progress under the enhanced follow-up mechanism." is also correct because monitored jurisdictions must provide periodic progress updates to FATF or the relevant FATF-Style Regional Body. These reports enable assessors to evaluate whether the jurisdiction is implementing the agreed reforms and achieving progress toward resolving the identified strategic deficiencies. Monitoring and reporting continue until FATF determines that the jurisdiction has completed its action plan and no longer requires increased monitoring. FATF describes these processes in its materials on high-risk and other monitored jurisdictions and its Methodology for assessing technical compliance and effectiveness.

QUESTION NO: 49

Release of the EU's Fourth AML Directive resulted in what change to member state*s procedures? (Select Two.)

A. The threshold for reporting suspicious transactions decreased from 15,000 EUR to 10,000 EUR.

B. All financial institutions were required to identify and verify the beneficial owner of legal entities.

C. Money laundering and terrorist financing were defined as separate crimes, expanding the directive's measures.

D. The scope of obliged entities was enlarged from casinos to all providers of gambling services.

E. Knowledge of criminal conduct could be inferred from objective factual circumstances.

ANSWER: B D

Explanation:

The EU’s Fourth Anti-Money Laundering Directive, Directive (EU) 2015/849, strengthened customer due diligence and widened the sectors subject to AML/CFT obligations. “All financial institutions were required to identify and verify the beneficial owner of legal entities” reflects the Directive’s requirement that obliged entities conduct customer due diligence, including identifying the beneficial owner and taking reasonable measures to verify that person’s identity when dealing with corporate or other legal-entity customers. This enhanced transparency was a central measure intended to prevent criminals from concealing ownership or control through legal persons and arrangements.

“The scope of obliged entities was enlarged from casinos to all providers of gambling services” also reflects a significant expansion. The Directive applies to providers of gambling services rather than limiting coverage to casinos. Member states may grant narrowly tailored, risk-based exemptions for certain gambling services where the risk is demonstrated to be low, but the baseline scope is broader. These changes required member states to implement more comprehensive procedures addressing beneficial ownership and gambling-sector AML/CFT controls. See Articles 2 and 13 of Directive (EU) 2015/849 on EUR-Lex and the European Commission’s overview of the EU AML/CFT framework.

QUESTION NO: 50

Assessing the money laundering risk related to a product within the financial sector includes assessing the: (Select Two.)

A. governance arrangements

B. complexity of the products

C. results of the last audit

D. financial status of the business

ANSWER: A B

Explanation:

“Governance arrangements” and “complexity of the products” are relevant considerations when assessing money-laundering risk associated with a financial product. Governance arrangements determine whether the institution has clear ownership, accountability, oversight, risk controls, and escalation processes for the product throughout its life cycle. Effective governance supports the identification, assessment, monitoring, and mitigation of risks arising from how the product is designed, approved, distributed, and used. Product complexity is also a key risk factor because features such as multiple transaction stages, opaque structures, rapid movement of value, cross-border functionality, or numerous intermediaries can make the source, ownership, and movement of funds more difficult to understand and monitor. A risk-based assessment should evaluate these characteristics in the context of the product’s intended purpose, customer base, delivery method, transaction limits, and geographic exposure. This approach aligns with the FATF risk-based framework, which expects financial institutions to identify and assess ML/TF risks and apply controls proportionate to those risks. See the FATF Recommendations and FATF's Risk-Based Approach for the Banking Sector.

QUESTION NO: 51

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:

It serves as the central agency for the receipt of disclosures filed by reporting entities. This describes a foundational function of a government Financial Intelligence Unit (FIU). Under Financial Action Task Force (FATF) Recommendation 29, an FIU serves as the national center for receiving suspicious transaction reports and other information relevant to money laundering, associated predicate offenses, and terrorist financing. The FIU analyzes these disclosures, together with other available information, to develop financial intelligence and disseminates that intelligence to competent authorities when the legal threshold for doing so is met. This centralization supports consistent handling of reports, protects the confidentiality of reporting, and enables analysts to identify links, patterns, transactions, and persons that may not be apparent from an individual report. The Egmont Group likewise defines an FIU as a national center responsible for receiving and analyzing disclosures and disseminating the results of that analysis. Although an FIU's precise powers and organizational location differ by jurisdiction, receiving disclosures from reporting entities is a core element of the internationally accepted FIU role. See FATF Recommendations, Recommendation 29 and the Egmont Group's description of FIUs.

QUESTION NO: 52

Which statements regarding the USA PATRIOT ACT best describe key aspects that have extraterritorial reach? (Choose three.)

A. It allows for the US Attorney General to subpoena records from a foreign bank with US correspondent accounts, including those that are located outside the US.

B. It requires foreign banks with US correspondent accounts to designate a registered agent in the US to accept service of subpoenas.

C. It allows the Secretary of the Treasury to order a US financial institution (FI) to close a correspondent account when a subpoena has not been responded by a foreign bank in a timely manner.

D. It obliges the government to trace the origin of the funds when a seizure of assets occurs in a correspondent account that has been opened and maintained for a foreign bank in the US.

E. It excludes as foreign FIs businesses that would be considered broker-dealers, money transmitters, and currency exchangers.

F. It allows federal banking supervisors to require records of the identity of the owners of a foreign bank from a FI operating in the US.

ANSWER: A B C

Explanation:

The correct statements describe the cross-border enforcement mechanisms in Section 319(b) of the USA PATRIOT Act, codified at 31 U.S.C. § 5318(k). The Act permits the Attorney General or Secretary of the Treasury to subpoena a foreign bank that maintains a correspondent account in the United States for records relating to that account, including records held outside the United States. This authority gives U.S. investigators access to information necessary to investigate money laundering and related financial crime when relevant records are maintained abroad.

Foreign banks with U.S. correspondent accounts must designate a U.S. resident agent to accept service of legal process, including subpoenas. This designation provides a practical and enforceable means of serving the foreign institution within U.S. jurisdiction. The statute also authorizes the Secretary of the Treasury or the Attorney General to direct a covered U.S. financial institution to terminate a foreign bank's correspondent account if the bank fails to comply with a subpoena or to challenge it in a U.S. court within the required period. Together, these measures condition access to the U.S. financial system on transparency, responsiveness, and cooperation with lawful U.S. investigations. See 31 U.S.C. § 5318 and FinCEN's USA PATRIOT Act resources.

QUESTION NO: 53

As emphasized in theBasel Committee guidancefor"Sound Management of Risks Related to Money Laundering and Financing of Terrorism", thethird line of defense (audit function)should:

A. Conduct AML audits no less often than every 12 months for consistency in annual reporting.

B. Report to the audit committee of the board of directors to maintain independence.

C. Remain independent from expressing opinions on the sufficiency of remediation or action plans to address findings and recommendations.

D. Be involved in the day-to-day operations of the AML program to immediately prevent control failures.

ANSWER: B

Explanation:

The correct answer is "Report to the audit committee of the board of directors to maintain independence." The third line of defense is the internal audit function, whose essential purpose is to provide objective, independent assurance on the adequacy and effectiveness of governance, risk management, and internal controls, including controls for money-laundering and terrorist-financing risk. Direct functional reporting to the board or its audit committee protects that independence by giving internal audit an escalation path outside the management structures and operational areas it reviews. This reporting relationship enables the audit committee to approve the audit charter and plan, consider significant findings, monitor management's response, and ensure that auditors have appropriate authority, access, and resources. In its guidance, the Basel Committee states that internal audit should be independent from the activities it audits and should report directly to the board of directors or its audit committee. For an AML/CFT framework, this independence supports credible testing of customer due diligence, transaction monitoring, sanctions-related controls, suspicious-activity reporting processes, and remediation of identified weaknesses. The board's audit committee can therefore use audit results as independent assurance when exercising its ultimate oversight responsibilities. See the Basel Committee's Sound management of risks related to money laundering and financing of terrorism and the Basel Committee's Corporate governance principles for banks.

QUESTION NO: 54

Which aspect of the USA PATRIOT Act impacts foreign financial institutions?

A. Requiring enhanced due diligence for foreign shell banks

B. Expanding sanctions requirements to a U.S. financial institution's foreign branches

C. Expanding the anti-money laundering program requirements to all foreign financial institutions

D. Providing authority to impose special measures on institutions that are of primary money-laundering concern

ANSWER: D

Explanation:

Providing authority to impose special measures on institutions that are of primary money-laundering concern is the relevant provision. Section 311 of the USA PATRIOT Act, codified at 31 U.S.C. § 5318A, authorizes the Secretary of the Treasury to determine that a foreign jurisdiction, foreign financial institution, class of international transactions, or type of account is of "primary money laundering concern." Following that finding, Treasury may impose one or more special measures. These range from enhanced recordkeeping and reporting requirements to requiring identification of beneficial owners for certain accounts, and may culminate in prohibiting or imposing conditions on U.S. financial institutions maintaining correspondent or payable-through accounts for the designated institution.

This authority has a direct practical impact on foreign financial institutions because access to correspondent banking relationships is often essential for U.S.-dollar transactions and participation in the international financial system. A special measure therefore can limit a targeted institution's ability to transact through U.S. banks, while also encouraging stronger transparency and AML controls. The statutory framework is designed to protect the U.S. financial system from identified money-laundering risks while using U.S. financial institutions' account relationships to address risks associated with foreign entities. See FinCEN's Section 311 Special Measures resource and 31 U.S.C. § 5318A.

QUESTION NO: 55

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

A. Regulation (EU) 2024/1624 of the European Parliament

B. Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases (COSMIC)

C. USA Patriot Act Section 314(a)

D. USA Patriot Act Section 314(b)

ANSWER: D

Explanation:

USA Patriot Act Section 314(b) is correct because it provides a voluntary information-sharing safe harbor that allows eligible financial institutions to share information with one another to identify and report potential money laundering and terrorist-financing activity. Before participating, an institution must submit a notice to FinCEN, the bureau of the U.S. Department of the Treasury that administers the program, and must take reasonable steps to verify that another participant has also submitted the required notice. The authority is implemented through FinCEN's regulations at 31 CFR § 1010.540. Information shared under this framework may be used only to identify and, where appropriate, report activities involving possible money laundering or terrorist activity. Participating institutions also receive protection from liability for information shared in good faith, provided they comply with the statutory and regulatory conditions. This mechanism supports stronger detection by enabling institutions to connect transactional or customer information that may appear unremarkable when viewed by a single institution alone. FinCEN's overview of the voluntary program is available at FinCEN Section 314(b), and the governing regulatory text is available through 31 CFR § 1010.540.

QUESTION NO: 56

What are the most effective measures to boost risk appetite awareness across an organization after a risk appetite has been set and a risk appetite statement (RAS) has been drafted? (Select Three.)

A. Provide training to staff so they understand the role risk appetite and its limits play in the safe conduct of business

B. Train all managers on the importance and benefits of "good" risk-taking

C. Embed the risk appetite into everyday processes and governance

D. Describe risk controls for business colleagues

E. Integrate misalignment with risk appetite into internal reporting procedures

ANSWER: A C E

Explanation:

Provide training to staff so they understand the role risk appetite and its limits play in the safe conduct of business, embed the risk appetite into everyday processes and governance, and integrate misalignment with risk appetite into internal reporting procedures. Together, these measures make the RAS an active management tool rather than a document that exists only at board or senior-management level.

Training translates approved risk boundaries into practical expectations for employees whose decisions affect customer acceptance, products, transactions, controls, and escalations. Embedding the appetite in governance and day-to-day processes ensures that approvals, delegated authorities, policies, performance oversight, and escalation routes consistently reflect the organization's stated tolerances. Internal reporting of actual or potential misalignment gives management and the board timely visibility into breaches, emerging concentrations, and the need for remediation or reassessment of limits. This supports clear accountability and informed risk decisions throughout the organization. The Financial Stability Board's risk-appetite principles emphasize communication, incorporation into decision-making, and reporting against risk appetite as essential elements of an effective framework. See the FSB Principles for an Effective Risk Appetite Framework and the Basel Committee guidance on corporate governance principles for banks.

QUESTION NO: 57

Whichpersons must always comply with all Office of Foreign Assets Control (OFAC) regulations? (Select Three.)

A. U.S. citizens regardless of location.

B. Non-U.S. financial institutions that offer accounts in USD regardless of location.

C. Merchants that offer U.S.-origin goods for sale regardless of location.

D. U.S.-incorporated entities and their foreign branches.

E. Permanent U.S. resident aliens regardless of location.

ANSWER: A D E

Explanation:

"U.S. persons" are the core group directly subject to OFAC-administered economic and trade sanctions. This category includes U.S. citizens regardless of location and permanent U.S. resident aliens regardless of location. Consequently, an individual's physical presence outside the United States does not remove the obligation to comply with applicable blocking, rejection, reporting, licensing, and transaction-prohibition requirements. U.S.-incorporated entities and their foreign branches are likewise U.S. persons for OFAC purposes and must maintain sanctions controls that prevent prohibited activity throughout their operations. This treatment of foreign branches is particularly important for multinational financial institutions and businesses because a branch is part of the same legal entity as its U.S.-organized parent. OFAC's guidance explains that sanctions programs generally apply to U.S. persons, defined to include U.S. citizens, permanent resident aliens, entities organized under U.S. law and their foreign branches, and persons located in the United States. The precise restrictions, licensing provisions, and reporting duties vary by sanctions program and transaction, but these persons remain within OFAC jurisdiction wherever they operate. See OFAC's FAQ on who must comply with OFAC regulations and its Sanctions Programs and Country Information.

QUESTION NO: 58

Who has the day-to-day responsibility of communicating and reinforcing the established anti-money laundering compliance culture and program?

A. Business lines

B. Senior management

C. Board of directors

D. Compliance officer

ANSWER: D

Explanation:

The compliance officer has the day-to-day responsibility for communicating and reinforcing the established anti-money laundering compliance culture and program. In practice, this individual—often designated the BSA officer, AML compliance officer, or money laundering reporting officer depending on the jurisdiction—administers the institution's AML framework and helps ensure that it operates consistently across the organization. This includes maintaining and communicating policies and procedures, coordinating appropriate training, overseeing monitoring and escalation processes, supporting investigations and regulatory reporting, and providing guidance to staff and business units on AML obligations.

An effective AML program requires more than written policies: employees must understand their responsibilities and apply controls in routine activities. The compliance officer is central to embedding those expectations operationally, monitoring whether the program remains effective, identifying weaknesses, and escalating material issues through the appropriate governance channels. This ongoing communication and reinforcement promotes a culture in which AML risk management is part of normal business conduct. The FFIEC describes the designated BSA compliance officer as responsible for coordinating and monitoring day-to-day BSA compliance. See the FFIEC BSA/AML Examination Manual and FinCEN's Bank Secrecy Act resources.

QUESTION NO: 59

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

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

A. Since the Basel Committee has no enforcement authority, it relies on the commitment of its members to carry out its guidance

B. Basel guidance includes standards to be incorporated into local legal frameworks, guidelines for implementation, and best-practice guidance

C. The Basel Committee's Core Principles include guidance on customer identification and acceptance

D. Members of the BCBS must implement its standards or face suspension from membership

E. The Basel Committee is composed of the 28 largest banks in the world

ANSWER: A B C

Explanation:

The BCBS develops global prudential standards and supervisory guidance, but it is not a treaty-based regulator with direct legal power over banks or jurisdictions. Its standards therefore depend on members' commitment to implement them through domestic legislation, regulation, and supervisory practice. The BCBS describes this approach as relying on its members' commitments and on monitoring implementation rather than on direct enforcement. Its publications include high-level standards, such as the Basel Framework and Core Principles, as well as supporting implementation guidance and sound-practice material that jurisdictions can use within their own legal and supervisory systems.

Customer due diligence is also an established part of the Committee's supervisory expectations. In the *Core Principles for Effective Banking Supervision*, the principle addressing abuse of financial services requires supervisors to determine that banks maintain policies and processes covering customer acceptance and identification, as well as ongoing monitoring of higher-risk accounts. These measures support effective risk management and help banks prevent their services from being used for criminal purposes, including money laundering and terrorist financing. See the BCBS overview at https://www.bis.org/bcbs/ and the Core Principles for Effective Banking Supervision.

QUESTION NO: 60

Which is a red flag for funds transfers?

A. Funds transfers are received in numerous small quantities from entities that are in related industries.

B. Funds transfers are repeatedly sent to the same beneficiary out of line with the business purpose.

C. Funds transfers are repetitive and within expected patterns.

D. Funds transfers are to a higher-risk geographic location with a known supplier within the same industry as the originator.

ANSWER: B

Explanation:

Funds transfers are repeatedly sent to the same beneficiary out of line with the business purpose. This is a funds-transfer red flag because transaction monitoring must assess activity in the context of the customer's expected profile, occupation or business model, stated purpose of the account, and known counterparties. Repeated transfers to one beneficiary may be legitimate when supported by a clear commercial relationship, but the lack of alignment with the customer's business purpose removes that apparent economic rationale and warrants investigation.

An institution should review the beneficiary relationship, payment narratives, invoices or contracts, transaction amounts and frequency, source of funds, and whether the activity is consistent with anticipated account use. Repetition can be significant because it may indicate that the beneficiary is being used to concentrate, move, or disguise funds through a recurring payment channel. The appropriate response is risk-based escalation and documentation of the review; where the complete facts create suspicion, the institution should consider filing a suspicious activity report in accordance with applicable requirements. The FFIEC's BSA/AML examination materials identify unusual wire-transfer activity and activity inconsistent with a customer's business as circumstances requiring scrutiny. FATF likewise emphasizes identifying transactions lacking an apparent economic or lawful purpose. See the FFIEC BSA/AML Examination Manual and FATF Recommendations.

QUESTION NO: 61

A country has completed a national assessment of money laundering and terrorist financing risks.

Which two actions should the country take to use the assessment effectively? (Choose two.)

A. Allocate resources and set priorities in line with identified risks.

B. Provide relevant risk information to reporting entities where appropriate.

C. Apply identical enhanced due diligence measures to every customer and sector.

D. Replace all customer due diligence requirements with the national risk assessment.

E. Restrict the assessment's use to law enforcement agencies.

ANSWER: A B

Explanation:

Allocating resources and setting priorities in line with identified risks is an appropriate use of a national risk assessment. The assessment should help competent authorities determine where supervisory, investigative, intelligence, policy, and enforcement resources are most needed. It can also identify sectors, products, geographic areas, and criminal threats requiring focused action.

Providing relevant risk information to financial institutions and designated non-financial businesses and professions is also important. Reporting entities need a sufficient understanding of national and sectoral risks to apply customer due diligence, monitoring, reporting, and other controls proportionately. Information sharing should be conducted in a manner that protects sensitive intelligence, investigations, and national-security interests. FATF Recommendation 1 requires countries to identify, assess, and understand their money laundering and terrorist financing risks and apply a risk-based approach. See the FATF Recommendations.

QUESTION NO: 62

Which section of the USA PATRIOT Act permits the US government to seize funds deposited in a US correspondent account of a foreign bank, creating extraterritorial impact?

A. Section 314(a)

B. Section 314(b)

C. Section 319(b)

D. Section 319(a)

ANSWER: D

Explanation:

Section 319(a) is correct. This provision, codified at 18 U.S.C. § 981(k), gives U.S. authorities a powerful forfeiture mechanism involving foreign banks' U.S. interbank, or correspondent, accounts. Where funds are subject to civil forfeiture and are held at a foreign bank, the statute permits the government to bring a forfeiture action against an equivalent amount of funds held in that foreign bank's interbank account at a covered financial institution in the United States. For forfeiture purposes, the funds are deemed to have been deposited in the United States, allowing U.S. jurisdiction even when the underlying illicit funds are located outside the country.

This mechanism creates the statute's important extraterritorial effect: a foreign bank's access to the U.S. correspondent-banking system may expose its U.S.-held account balance to seizure based on funds connected to criminal activity abroad. The provision also contains protections concerning innocent owners and the relationship between the funds forfeited and the foreign bank's U.S. interbank account. The statutory text is available at [18 U.S.C. § 981]. FinCEN's correspondent-account rules and related framework are available at [31 C.F.R. § 1010.610].

QUESTION NO: 63

A real estate buyer purchases multiple high-value properties in cash through a series of transactions in a short period of time and without any clear economic justification.

Which of the following is the most likely money laundering risk associated with this behavior in the real estate sector?

A. The buyer is using high-value real estate transactions to obscure the origin of the funds.

B. The buyer is quickly diversifying their investment portfolio through structuring payments in order to take advantage of the liquidity of cash transactions in real estate.

C. The buyer is capitalizing on favorable market conditions and using cash purchases to outbid competitors in a competitive real estate market using insider information.

D. The buyer is a real estate developer acquiring multiple properties for a potential redevelopment project with a business partner located in a high-risk jurisdiction.

ANSWER: A

Explanation:

The buyer is using high-value real estate transactions to obscure the origin of the funds. Real estate is attractive for money launderers because it can absorb substantial amounts of illicit proceeds in a single asset class, potentially convert criminal cash into apparently legitimate wealth, and provide a basis for later resale or borrowing against the property. Multiple high-value cash acquisitions within a short period, particularly where the activity lacks a credible economic purpose, are important indicators that the transactions may be intended to place and integrate illicit funds rather than meet a genuine investment or housing need.

Cash reduces the transparency available from regulated financial institutions and can make it more difficult to establish a complete source-of-funds trail. Repeated purchases can also create layers of transactions and ownership that complicate efforts to identify the true source of wealth and the beneficial owner. Accordingly, this pattern calls for enhanced scrutiny of the buyer's identity, beneficial ownership, source of wealth, source of funds, transaction rationale, and any connections among the purchases. FATF identifies the use of real estate to conceal or integrate illicit proceeds as a material vulnerability and emphasizes risk-based due diligence and reporting where suspicious indicators are present. See FATF's report on real-estate ML/TF risks and the FATF Recommendations.

QUESTION NO: 64

Pursuant to the Third European Union Money Laundering Directive, how long after being out of prominent office should a person NOT be considered to be a

Politically Exposed Person (PEP)?

A. 1 year

B. 2 years

C. 3 years

D. 4 years

ANSWER: A

Explanation:

1 year is the applicable period under the Third EU Money Laundering Directive. The Directive required financial institutions and other covered entities to continue treating a person who had ceased to hold a prominent public function as a PEP for *at least* one year. This reflects the fact that the influence, access, relationships, and corruption exposure arising from a prominent public role may continue after the formal role ends.

Importantly, the one-year period is a minimum rather than an automatic point at which all PEP-related risk ends. After that period, institutions must apply a risk-sensitive approach in deciding whether enhanced due diligence remains appropriate. Relevant considerations can include the former official's seniority, continuing political or commercial influence, the nature of the jurisdiction, links to state-controlled entities, and the customer's products, transactions, or source of wealth. Thus, one year is the Directive's specified post-office baseline, while a financial institution may continue enhanced measures when its risk assessment supports doing so.

This requirement appears in Article 3(9) of Directive 2005/60/EC. The European Commission's EU AML/CFT framework overview provides further context for the EU's risk-based AML/CFT regime.

QUESTION NO: 65

Using the customer profile and expected activity information, a financial institution should be able to identify transactions that are difficult to:

A. make economic sense

B. make viable profitability.

C. be strategically viable.

D. cross verify.

ANSWER: A

Explanation:

The correct completion is "make economic sense." A customer profile, established through customer due diligence and refreshed through ongoing due diligence, gives the institution a reasonable baseline for the customer's occupation or business, anticipated account usage, source of funds, expected counterparties, transaction sizes, products, and geographic exposure. Comparing actual activity against that baseline enables the institution to recognize transactions that lack an apparent economic or lawful purpose. For example, payments that move rapidly among unrelated parties, transfers that are inconsistent with the customer's stated business operations, or unusual movements of funds with no credible commercial rationale may be difficult to make economic sense and therefore warrant review.

This principle supports effective transaction monitoring: alerts should be assessed in the context of what is known about the customer, with investigators seeking a reasonable explanation and supporting information for anomalous activity. Where the institution knows, suspects, or has reason to suspect that funds involve illicit activity, are intended to hide such activity, or otherwise meet applicable reporting thresholds, the matter may require escalation and suspicious activity reporting. FATF Recommendation 10 requires ongoing due diligence and scrutiny of transactions to ensure they are consistent with the institution's knowledge of the customer, business, and risk profile. See the FATF Recommendations and FinCEN's Suspicious Activity Reporting guidance.

QUESTION NO: 66

The compliance officer for a private bank has been tasked with writing a policy on how the bank will deal with intermediaries.

Which two aspects should be included in the policy in respect of intermediaries to align it with the Wolfsberg Anti-Money Laundering Principles for Private Banking? (Choose two.)

A. When an intermediary introduces clients to the bank, it is not necessary for the bank to perform due diligence on the intermediary's clients.

B. Where an intermediary introduces clients to the bank, the bank must obtain the same type of information with respect to an introduced client that would otherwise be obtained by the bank, absent the involvement of the intermediary.

C. Where an intermediary manages assets on behalf of a number of clients and is the account holder with the bank, but that intermediary does not conduct the same level of due diligence as the bank, it is necessary for the bank to undertake due diligence on the intermediary's clients.

D. Where an intermediary manages assets on behalf of a number of clients and arranges for the opening of accounts for its clients with the bank, and that intermediary is a financial institution subject to similar regulations, it is necessary for the bank to perform due diligence on the intermediary's clients.

ANSWER: B C

Explanation:

"Where an intermediary introduces clients to the bank, the bank must obtain the same type of information with respect to an introduced client that would otherwise be obtained by the bank, absent the involvement of the intermediary" is correct because use of an introducer does not transfer the private bank's responsibility for customer due diligence. The bank's policy must ensure that it has sufficient information to identify and verify the client and beneficial owner, understand the purpose of the relationship, assess risk, and conduct ongoing monitoring to its normal standard. The information may be collected through the intermediary in appropriate circumstances, but the bank remains responsible for ensuring its due-diligence requirements are satisfied.

"Where an intermediary manages assets on behalf of a number of clients and is the account holder with the bank, but that intermediary does not conduct the same level of due diligence as the bank, it is necessary for the bank to undertake due diligence on the intermediary's clients" is also correct. In this arrangement, the intermediary may obscure the underlying clients from the bank. Wolfsberg principles require a risk-based approach that considers the intermediary's controls and the extent to which they are equivalent. If those controls are not comparable, the bank must obtain sufficient transparency and due diligence on underlying clients to manage the resulting money-laundering and terrorist-financing risk. See the Wolfsberg FAQs on Intermediaries and the Wolfsberg AML Principles for Private Banking.

QUESTION NO: 67

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

A. Use of mortgage products

B. Use of commercial properties inconsistent with stated business purposes

C. Use of complex loans or credit finance

D. Use of corporate vehicles or complex ownership structures

E. Unexplained cash payments

F. Use of agricultural land in rural areas

ANSWER: B C D E

Explanation:

The Financial Action Task Force identifies real estate as attractive for laundering illicit proceeds because transactions can involve high values, opaque funding arrangements, and legal entities that obscure the persons ultimately controlling an asset. “Use of commercial properties inconsistent with stated business purposes” is a meaningful indicator because a property’s acquisition, occupancy, or financial activity may lack a credible commercial rationale. “Use of complex loans or credit finance” can indicate an effort to disguise the source of funds, create a paper trail that appears legitimate, or move value through unusual financing arrangements. “Use of corporate vehicles or complex ownership structures” is relevant because layered companies, trusts, nominees, and cross-border structures can conceal beneficial ownership and impede customer due diligence. “Unexplained cash payments” are also a significant concern, particularly where the amount, method, or source of cash is inconsistent with the customer profile, transaction, or local market practice. These indicators are risk signals requiring appropriate scrutiny; they do not independently establish that money laundering has occurred. FATF’s real-estate risk analysis emphasizes the need for reporting entities and relevant professionals to understand transaction context, source of funds, beneficial ownership, and unusual features of the deal. See the FATF report on money laundering through the real estate sector and FATF’s methods and trends resources.

QUESTION NO: 68

Which two protections should be available under the Financial Action Task Force standards to support suspicious transaction reporting? (Choose two.)

A. Protection from criminal and civil liability for good-faith suspicious transaction reporting.

B. A prohibition on disclosing that a suspicious transaction report has been filed.

C. Immunity from all regulatory obligations after a suspicious transaction report is filed.

D. A requirement to notify the customer before submitting a suspicious transaction report.

ANSWER: A B

Explanation:

Financial institutions, their directors, officers, and employees should be protected from criminal and civil liability for reporting suspicions in good faith, even when they do not know precisely what underlying criminal activity occurred. This protection supports timely reporting and reduces the risk that legitimate concerns will be suppressed because of fear of liability for breach of confidentiality or other restrictions.

Countries should also prohibit financial institutions and their directors, officers, and employees from disclosing that a suspicious transaction report or related information has been filed with the financial intelligence unit. This prohibition protects the integrity of financial intelligence, avoids alerting subjects of an inquiry, and reduces the risk of evidence destruction or flight. These safeguards are reflected in FATF Recommendation 21. See the FATF Recommendations.

QUESTION NO: 69

Which actions should a compliance officer take when implementing an enterprise-wide approach to managing money laundering risks in institutions operating with multiple lines of business and in various jurisdictions? (Choose three.)

A. Design systematic controls specific to local regulatory expectations.

B. Create processes to obtain and review information in accordance with its global anti-money laundering policies and procedures.

C. Adopt policies and procedures that comply with relevant laws and work to identify, monitor, and mitigate group-wide risks.

D. Institute a risk-based approach utilizing the most recent risk assessment of only the head office.

E. Establish jurisdiction centric committees where relevant laws are reviewed and analyzed to understand their impact on the organization.

F. Implement a comprehensive baseline for managing risks by administering a process that applies policies and procedures on a group-wide basis.

ANSWER: B C F

Explanation:

"Create processes to obtain and review information in accordance with its global anti-money laundering policies and procedures" is essential because effective enterprise-wide oversight depends on timely, reliable information flowing across business lines and entities. This allows the group to identify risks that may not be apparent when customer relationships, transactions, and control findings are viewed only locally.

"Adopt policies and procedures that comply with relevant laws and work to identify, monitor, and mitigate group-wide risks" correctly combines consolidated financial-crime risk management with compliance in each applicable jurisdiction. A group framework must support consistent governance, risk identification, escalation, and mitigation while being implemented in a manner that meets relevant legal and regulatory obligations.

"Implement a comprehensive baseline for managing risks by administering a process that applies policies and procedures on a group-wide basis" establishes common minimum AML standards across the organization. FATF expects financial groups to maintain group-wide AML/CFT programmes, including policies and procedures for information sharing and risk management, with appropriate safeguards. The Basel Committee likewise emphasizes group-wide management of money-laundering and terrorist-financing risks across a banking group. These measures create consolidated visibility and consistent control expectations while supporting jurisdiction-specific implementation. See FATF Recommendations and Basel Committee guidance on AML/CFT risk management.

QUESTION NO: 70

Which activities could be considered a potential spear phishing scam? (Select Three.)

A. An employee receives a phone call requesting that money be sent to assist someone in trouble.

B. A courier delivers a duplicate invoice to a business that contains updated payment details of an existing supplier.

C. Payroll receives an external email from an employee looking to update their bank account information.

D. A business sends its employees an email warning that email passwords must be changed to prevent cyber-fraud.

E. An employee receives an email that asks to download an attachment, but the attachment is a malware.

F. Members of a religious organization receive a donation request by email claiming to be from their leader.

ANSWER: B C E

Explanation:

Spear phishing is a targeted social-engineering attack that exploits a known relationship, business process, or recipient role to induce an action that benefits a fraudster. "A courier delivers a duplicate invoice to a business that contains updated payment details of an existing supplier" reflects supplier-impersonation or invoice-diversion fraud. The request leverages the established vendor relationship and a seemingly routine accounts-payable process to redirect legitimate payments to an account controlled by criminals. "Payroll receives an external email from an employee looking to update their bank account information" is a targeted business-email-compromise scenario: payroll staff are specifically selected because they can alter payment instructions, allowing an attacker impersonating an employee to divert wages. "An employee receives an email that asks to download an attachment, but the attachment is a malware" is also a potential spear phishing attempt when the message is directed at a particular employee and uses a malicious attachment to obtain access, steal data, or deploy malware. These scenarios illustrate the key control principle of independently verifying changed payment instructions and unexpected attachments through a trusted channel before acting. ACAMS identifies phishing and social engineering as techniques criminals use to obtain access or facilitate fraud; see the ACAMS Financial Crime Glossary. Guidance from the U.S. Cybersecurity and Infrastructure Security Agency likewise emphasizes that targeted phishing messages may impersonate trusted people or organizations and seek to trigger payment, credential, or attachment-related actions.

QUESTION NO: 71

Which regulation regarding data privacy has to be considered while carrying out a financial crime investigation?

A. General Data Protection Regulation

B. European Enforcement Order

C. Securities Financing Transactions Regulation

D. Rome II Regulation

ANSWER: A

Explanation:

The General Data Protection Regulation is the principal EU data-privacy framework to consider when a financial crime investigation involves processing personal data. Investigative activity commonly requires the collection, review, analysis, sharing, and retention of customer due-diligence records, account and transaction information, communications, internal alerts, and case-management notes. The General Data Protection Regulation governs such processing where it occurs in the EU/EEA and may also apply to certain processing by organizations outside that area involving individuals in the EU. It requires organizations to identify an appropriate lawful basis for processing and to apply core principles including purpose limitation, data minimization, accuracy, storage limitation, and appropriate security and confidentiality safeguards. In an AML/CFT context, processing will frequently be necessary for compliance with a legal obligation under applicable anti-money-laundering law. Investigators and their institutions should therefore ensure that access is limited to authorized personnel, evidence and case files are secured, disclosures are controlled and documented, and records are retained only for legally required or otherwise justified periods. The regulation also requires accountability: organizations must be able to demonstrate that their investigative-data practices comply with applicable requirements. The official text is available at EUR-Lex: Regulation (EU) 2016/679; practical EU context is provided by the European Commission's data-protection guidance.

QUESTION NO: 72

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 an international network of financial intelligence units that strengthens members' capacity to combat money laundering, related predicate offences, and terrorist financing through practical cooperation. "Provides support to expand and systematize cooperation related to the reciprocal exchange of information" reflects a central Egmont objective:

enabling FIUs to exchange financial intelligence efficiently and on a reciprocal basis across borders. This cooperation helps FIUs connect information held in different jurisdictions and supports timely analysis of suspicious activity.

"Fosters better and secure communication through the application of technology" is also correct because the Egmont Secure Web provides a protected channel for FIU-to-FIU communication and information exchange. Secure communications are essential because financial intelligence is sensitive and must be shared subject to confidentiality, legal, and operational safeguards.

"Encourages operational autonomy of financial intelligence units" is correct because effective FIUs need sufficient independence and autonomy to receive, analyze, and disseminate financial intelligence without improper influence. Egmont promotes the development and effectiveness of FIUs, including sound operational standards, cooperation, training, and information-sharing practices. These functions directly support members' ability to perform their intelligence role. See the Egmont Group's mission and objectives and FATF's Recommendations, particularly the standards concerning FIUs and international cooperation.

QUESTION NO: 73

The Head of Compliance was informed by external auditors of a finding that indicates an element of AML policy failed to comply with the regulatory requirement. Which action should the Head of Compliance take next?

A. Make necessary updates to AML policy documents.

B. Inform the compliance team about the finding.

C. Agree immediately and provide corrective actions.

D. Submit a corrective action plan with a target timeline.

ANSWER: D

Explanation:

Submitting a corrective action plan with a target timeline is the appropriate next step because it establishes a documented, accountable process for restoring compliance after an independent audit identifies a regulatory deficiency. An effective plan should first confirm the scope and root cause of the policy failure, then define the remediation required to bring the policy and its implementation into alignment with the applicable requirement. It should assign a responsible owner, identify necessary resources and controls, set measurable milestones and a realistic completion date, and provide for progress tracking and validation that remediation is effective. This approach enables senior management, auditors, and—where reporting or supervisory engagement is required—the relevant regulator to understand how the institution will resolve the issue and prevent recurrence. It also supports the continuing effectiveness of the institution's AML program, which must include internal controls designed to ensure ongoing compliance with Bank Secrecy Act requirements. The regulatory AML-program standard is available at 31 CFR 1020.210. The FFIEC BSA/AML Examination Manual also emphasizes independent testing and management's attention to identified compliance weaknesses; see the FFIEC assessment of BSA regulatory compliance.

QUESTION NO: 74

When deciding on the frequency of periodic customer due diligence (CDD) refresh, firms should foremost consider the:

A. Risk profile of customers

B. Available level of automation for the process

C. Operational burden of periodic refresh implementation

D. Cost of implementation

ANSWER: A

Explanation:

The **Risk profile of customers** should foremost determine how frequently a firm refreshes customer due diligence information. A risk-based approach requires firms to apply enhanced scrutiny and more frequent reviews to relationships that present greater money-laundering, terrorist-financing, sanctions, corruption, or other financial-crime risk. Relevant factors include customer type and ownership structure, products and services used, expected transaction activity, geographic exposure, delivery channel, and adverse information. Conversely, lower-risk relationships may generally be reviewed less often, provided the firm continues to monitor activity and refreshes information when a triggering event or material change occurs. This approach ensures CDD resources are directed toward the relationships where updated information is most necessary to understand and mitigate risk, rather than applying a uniform timetable driven by process convenience. The Financial Action Task Force states that customer due diligence should be conducted on an ongoing basis, including scrutiny of transactions and ensuring documents, data, and information are kept up to date, particularly for higher-risk customer categories. U.S. regulatory guidance similarly emphasizes that customer risk profiles are dynamic and should be updated as risk-relevant information changes. See the FATF Recommendations and the FFIEC Customer Due Diligence guidance.

QUESTION NO: 75

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

A. The Financial Action Task Force (FATF)

B. The AUSTRAC Fintel Alliance

C. The Egmont Group

D. The Wolfsberg Group

ANSWER: B

Explanation:

The AUSTRAC Fintel Alliance is a well-established public-private partnership because it formally brings together Australia's financial intelligence agency, law-enforcement and national-security bodies, and regulated private-sector entities. Its purpose is operational: participants share intelligence, expertise, and analytical capabilities to identify, prevent, and disrupt serious financial crime. This collaborative structure enables government agencies to benefit from financial-sector insight and data, while private-sector participants receive typology information and strategic intelligence that can strengthen transaction monitoring, customer-risk assessment, and suspicious-matter reporting. AUSTRAC describes Fintel Alliance as a partnership involving major financial institutions and government agencies that works to combat money laundering, terrorism financing, and other serious crime. It is therefore a practical example of the kind of information-sharing partnership promoted internationally as an effective tool against financial crime, rather than merely an intergovernmental standard-setting body or an industry association. Its continuing operations and documented disruption outcomes demonstrate the sustained, action-oriented collaboration associated with a successful PPP. See AUSTRAC's Fintel Alliance overview and the Financial Action Task Force's public-private partnership resources.

QUESTION NO: 76

How do nominees benefit criminals misusing thorn for money laundering purposes? (Select Two.)

A. Allow beneficial owners to provide proxies lot voting on corporate decisions

B. Obscure beneficial ownership

C. Allow domicile in the nominee's jurisdiction

D. Derail investigations

ANSWER: B D

Explanation:

Obscure beneficial ownership is correct because nominee shareholders and directors can appear in corporate records as the legal owners or controllers while acting on behalf of the true beneficial owner. This separation between the person named in public or financial-institution records and the person who ultimately owns, controls, or benefits from the entity can conceal the source and destination of illicit funds. Effective customer due diligence therefore requires institutions to identify and verify the natural person who ultimately owns or controls a customer, rather than relying solely on nominal legal ownership.

Derail investigations is also correct because nominees can create misleading ownership and control trails. Investigators, financial institutions, and competent authorities may initially encounter nominee names, nominee addresses, and intermediary documentation instead of the individual directing transactions. This can delay efforts to trace assets, obtain relevant records, identify connected entities, and establish who exercised effective control. The Financial Action Task Force identifies nominee arrangements as a mechanism that can be used to conceal beneficial ownership and emphasizes the need for accurate, adequate, and timely beneficial-ownership information. See the FATF beneficial ownership guidance and FinCEN beneficial ownership information guidance.

QUESTION NO: 77

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

Which approach is the best option?

A. Only commit to action plans that require no new investment to maximize shareholder value

B. Draft action plans in consultation with the jurisdiction ' s FIU to remain aligned with other similar companies

C. Only commit to action plans that can be implemented and closed within the three-month management reporting cycle

D. Draft action plans to address the root cause of the deficiencies, regardless of how long they will take to fully implement

ANSWER: D

Explanation:

Draft action plans to address the root cause of the deficiencies, regardless of how long they will take to fully implement is the best approach because an effective remediation program must resolve the underlying control, governance, process, staffing, data, or technology failure identified by the independent audit. A plan focused only on quick closure or limited cost may leave the institution exposed to the same AML risk and result in repeat audit findings. Remediation should be risk-based and include a clearly defined corrective action, accountable owner, milestones, required resources, validation criteria, and escalation or reporting to senior management and the board as appropriate. Although implementation time frames should be realistic, the need for sustained remediation does not diminish merely because a corrective action extends beyond a routine reporting cycle. The compliance officer should ensure that interim controls are used where necessary while the permanent solution is being implemented, and that completion is independently validated before the issue is closed. This approach supports the expectation that independent testing findings lead to meaningful improvements in the AML program's effectiveness. The FFIEC BSA/AML examination guidance discusses independent testing and reporting of identified deficiencies to management for corrective action: FFIEC BSA/AML Manual. FATF also emphasizes effective, risk-based AML/CFT measures and ongoing assessment of their effectiveness: FATF Recommendations.

QUESTION NO: 78

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:

Lawyers are particularly vulnerable because legal professionals can provide access to activities that criminals seek to conduct under a false, stolen, or concealed identity. Their work may involve forming companies and trusts, managing client money, supporting property or corporate transactions, and acting for clients in dealings with financial institutions and public authorities. In these circumstances, an individual using fraudulent identity documents or an impersonated identity may seek to establish a legal person, obscure the true beneficial owner, or add apparent legitimacy to transactions and assets derived from crime.

For AML purposes, lawyers are commonly treated as professional intermediaries or "gatekeepers." Effective controls therefore require understanding the client's identity, verifying that identity using reliable information, determining whether someone else ultimately owns or controls the client or transaction, and scrutinizing unusual activity throughout the professional relationship. These measures reduce the risk that legal services are used to mask the persons behind funds, entities, or assets. OECD integrity work recognizes the importance of preventing misuse of professional intermediaries, while FATF's risk-based guidance addresses the identity, beneficial-ownership, and transaction risks facing legal professionals. See the OECD's anti-corruption and integrity resources and FATF guidance for legal professionals.

QUESTION NO: 79

Which technologies are commonly used to help financial institutions (FIs) navigate privacy and data protection regulations while securely sharing client information with private third-party entities? (Choose two.)

A. Blockchain to ensure traceability and security in shared data transactions

B. Data encryption to protect sensitive information from unauthorized access

C. Privacy-enhancing technologies (PETs) to enable secure and privacy-compliant data sharing

D. Artificial intelligence (AI) to automating compliance processes like data anonymization and secure sharing

E. Cloud storage solutions for efficient data handling and management

ANSWER: B C

Explanation:

Data encryption to protect sensitive information from unauthorized access is correct because encryption converts client data into a form that cannot be read without the appropriate cryptographic key. Financial institutions can apply encryption both while data are transmitted to a third party and while they are stored, reducing the risk that intercepted, lost, or improperly accessed information is exposed. Encryption is therefore a foundational technical safeguard supporting confidentiality and secure information sharing. The UK Information Commissioner's Office describes encryption as an appropriate technical measure for protecting personal data: ICO encryption guidance.

Privacy-enhancing technologies (PETs) to enable secure and privacy-compliant data sharing is also correct. PETs encompass methods such as de-identification, pseudonymisation, secure multiparty computation, and privacy-preserving analytics. These approaches can allow an FI and an approved third party to derive needed insights, conduct screening, or perform analysis while minimizing disclosure of directly identifiable client information. This supports data-minimization, purpose-limitation, and confidentiality expectations that are central to privacy compliance programs. The UK Information Commissioner's Office explains how PETs can enable organizations to use and share data while reducing privacy risks in its PETs guidance.

QUESTION NO: 80

A startup virtual currency exchange has registered as a money services business and will commence operations in six months. The company will provide digital wallets to customers to hold their virtual currency after purchase. Customers will have the option to conduct purchases of the virtual currency and transfer the currency to and from the digital wallet. The startup must develop an anti-money laundering compliance program prior to launch.

Which two anti-money laundering responsibilities should be considered before business launch? (Choose two.)

A. A customer onboarding process

B. Transaction limits consistent with risk appetite

C. Employees to handle complaints in a timely fashion

D. Mechanisms to monitor and protect customers' digital wallets from cyber-attacks

ANSWER: A B

Explanation:

A customer onboarding process and transaction limits consistent with risk appetite are key controls that should be designed and operational before the exchange begins serving customers. As a money services business, the exchange must maintain a written, risk-based anti-money laundering program with internal controls reasonably designed to prevent money laundering and to support Bank Secrecy Act compliance. Customer onboarding establishes the information and risk profile needed to apply appropriate due diligence, screen for applicable sanctions concerns, identify higher-risk relationships, and create a meaningful baseline for ongoing transaction monitoring.

Transaction limits translate the firm's risk assessment into product-level controls. Limits can be calibrated by factors such as customer risk, verification status, transaction type, velocity, funding or withdrawal method, and exposure to higher-risk jurisdictions. They help ensure that the exchange's wallet and transfer functionality operates within the monitoring, investigation, and suspicious-activity reporting capacity available at launch. These controls should be documented, tested, and governed as part of the firm's internal-control framework, with escalation processes for unusual activity. FinCEN identifies administrators and exchangers of convertible virtual currency as money transmitters in relevant circumstances and therefore subject to applicable MSB obligations. See [31 CFR § 1022.210] and [FinCEN's convertible virtual currency guidance].

QUESTION NO: 81

Which of the following accurately describes the economic, reputational and social consequences of money laundering (ML) and the risks and consequences of violating AFC regulations? (Choose two.)

A. ML undermines the integrity and stability of financial systems and makes them vulnerable to illegal activity. This can erode investor confidence and hinder economic growth.

B. When a financial institution (FI) is found to be promoting ML or violating AFC regulations, this can lead to a loss of confidence in the institution and a loss of customers. Interestingly, this scenario might sidestep any legal consequences for the FI.

C. When laundered funds flow into legitimate economies, they can be used for illegal purposes, such as funding terrorist activities or organized crime. This distorts resource allocation and undermines development.

D. Jurisdictions perceived as having insufficient ML measures might be identified as uncooperative or high-risk, potentially facing restricted access to international markets, though economic sanctions by other countries are an unlikely outcome.

ANSWER: A C

Explanation:

"ML undermines the integrity and stability of financial systems and makes them vulnerable to illegal activity. This can erode investor confidence and hinder economic growth." is correct because money laundering compromises the sound functioning and perceived trustworthiness of financial institutions and markets. When criminal proceeds enter the financial system, they can distort financial activity, increase exposure to crime and misconduct, and weaken confidence among customers, investors, counterparties, and international market participants. Reduced confidence can impair investment and thereby hinder sustainable economic development. The Financial Action Task Force (FATF) recognizes that money laundering threatens the integrity of the financial system and can have wider economic effects.

"When laundered funds flow into legitimate economies, they can be used for illegal purposes, such as funding terrorist activities or organized crime. This distorts resource allocation and undermines development." is also correct. Laundering enables criminals to retain, conceal, move, and deploy illicit proceeds, including in support of organized criminal enterprises and terrorism. Criminal capital may be directed toward activity based on concealment or criminal benefit rather than productive economic value, distorting competition and allocation of resources. Effective anti-financial-crime controls therefore protect both the financial system and broader social and economic development. See the FATF's description of its work and the IMF's AML/CFT resources.

QUESTION NO: 82

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

A. Receiving and analyzing Suspicious Activity Reports (SARs) to detect financial crime

B. Disseminating information on emerging trends related to money laundering and associated predicate offenses

C. Assisting financial institutions with designing products and services that lower residual money laundering risk

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

ANSWER: A B

Explanation:

Financial Intelligence Units are central to a jurisdiction's anti-money laundering and counter-terrorist financing framework because they turn reports and other relevant information into actionable financial intelligence. Receiving and analyzing Suspicious Activity Reports (SARs) to detect financial crime is a core FIU function. FIUs receive disclosures from reporting entities, assess the information using available financial, administrative, and—in appropriate circumstances—law-enforcement data, and identify transactions, relationships, patterns, and indicators that may warrant further attention by competent authorities.

Disseminating information on emerging trends related to money laundering and associated predicate offenses also supports financial integrity. FIUs disseminate operational intelligence when analysis identifies matters relevant to investigations, and may produce strategic intelligence that identifies methods, typologies, vulnerabilities, and developing risks. Sharing this intelligence helps law-enforcement and other competent authorities prioritize resources and helps reporting entities recognize evolving financial-crime indicators. FATF Recommendation 29 specifies that an FIU should serve as the national centre for receiving and analysing suspicious transaction reports and other relevant information, then disseminating the results of that analysis. See FATF Recommendations and the Egmont Group overview of FIUs.

QUESTION NO: 83

Financial Intelligence Units (FIUs) are responsible for:

A. the timely dissemination of cases to law enforcement agencies.

B. responding to requests from law enforcement agencies for information contained in regulatory reports.

C. sharing evidence with other FIUs.

D. receiving confirmed reports about committed crimes from accountable and reporting institutions.

ANSWER: A

Explanation:

The timely dissemination of cases to law enforcement agencies is correct because dissemination of financial intelligence is a central, defining FIU function. Under the FATF framework, an FIU serves as the national center for receiving disclosures concerning suspected proceeds of crime and potential terrorist financing, analyzing those disclosures and related information, and disseminating the results of that analysis. Dissemination enables competent authorities, particularly law enforcement, to use actionable intelligence to begin, support, prioritize, or broaden criminal investigations.

This role is not limited to merely passing along raw reports. An FIU adds value by evaluating suspicious transaction or activity reports, identifying connections, examining financial patterns, and producing intelligence that highlights potential money laundering, predicate offenses, or terrorist-financing concerns. Timeliness matters because funds can be moved rapidly, dissipated, or transferred across borders; prompt intelligence sharing can support asset tracing, restraint, and investigative action. The Egmont Group similarly describes FIUs through the core functions of receiving, analyzing, and disseminating financial intelligence. This receive-analyze-disseminate model is therefore the best single description of an FIU's responsibility. See [FATF Recommendation 29] and the [Egmont Group's description of FIUs].

QUESTION NO: 84

Which is a key role of FATF-Style Regional Bodies (FSRBs)?

A. Support the system of mutual evaluation

B. Setting regional standards for combatting money laundering

C. Bring additional terrorist financing laws into action in the region

D. Enforce the specific FATF laws in the region

ANSWER: A

Explanation:

Support the system of mutual evaluation is correct because FATF-Style Regional Bodies are regional associate members and partners in the global AML/CFT network whose core function is to promote implementation of the FATF Recommendations among their members. A central way they do this is through mutual evaluations: peer-based assessments that examine a jurisdiction's technical compliance with the FATF Recommendations and the effectiveness of its AML/CFT framework. FSRBs conduct or support these assessments using the common FATF Methodology, helping ensure that countries beyond FATF's direct membership are reviewed against a consistent international benchmark.

FSRBs also maintain follow-up processes after evaluations, encourage jurisdictions to remedy identified deficiencies, and support regional cooperation, training, and typologies work. These activities strengthen the practical application of global standards and provide FATF with regionally informed insight into money-laundering, terrorist-financing, and proliferation-financing risks. The FATF identifies mutual evaluation as a principal component of the work undertaken by its regional bodies, which collectively extend the reach and consistency of the worldwide AML/CFT assessment framework. See the [FATF overview] and its description of [FATF-Style Regional Bodies].

QUESTION NO: 85

What are the primary sources of reference besides AML laws and regulations when developing and maintaining the AML policies, standards, and procedures of a bank? (Choose three.)

A. National Risk Assessment

B. Regulatory guidance or publications

C. Government or state-run newspapers

D. Guidance issued by international bodies

E. Policies and procedures developed by other banks

ANSWER: A B D

Explanation:

National Risk Assessment, **Regulatory guidance or publications**, and **Guidance issued by international bodies** are primary reference sources for a bank's AML framework in addition to binding legal and regulatory requirements. A National Risk Assessment identifies material money-laundering and terrorist-financing threats, vulnerabilities, and risk priorities within the country. A bank can use those findings to calibrate its enterprise-wide risk assessment, customer due diligence, transaction-monitoring scenarios, escalation processes, and allocation of compliance resources. Regulatory guidance and publications provide supervisory expectations and practical interpretive direction that help institutions operationalize applicable requirements and respond to current typologies, enforcement themes, and identified control weaknesses. International guidance—particularly the Financial Action Task Force's risk-based approach and recommendations—supports alignment with globally recognized AML/CFT principles, cross-border risk awareness, and sound control design. These sources should be incorporated into a documented, risk-based governance process and reviewed as risks, products, customers, geographies, and supervisory expectations evolve. The FATF explains the international AML/CFT standards and risk-based approach in its Recommendations. In the United States, FinCEN publishes National Risk Assessments and related materials at its National Risk Assessments page.

QUESTION NO: 86

Which key financial crime risks relate to the remote gambling sector specifically? (Select Three.)

A. Customers not being physically present for identification purposes

B. Customers depositing large amounts of cash

C. Customers using anonymous prepaid cards

D. Customers betting more than they can afford

E. Customers making numerous low-level transactions to avoid enhanced due diligence

ANSWER: A C E

Explanation:

Customers not being physically present for identification purposes is a key remote-gambling risk because online operators must establish and verify identity without an in-person encounter. This creates greater exposure to impersonation, stolen or synthetic identities, account takeovers, and misuse of accounts by third parties. Effective remote onboarding therefore requires reliable electronic verification, authentication, and ongoing scrutiny appropriate to the customer and product risk. Customers using anonymous prepaid cards is also a material concern where a payment instrument obscures the source of funds or makes it difficult to establish the person controlling the payment. Gambling accounts can otherwise be used to place bets, move value, and withdraw apparently legitimate proceeds. Customers making numerous low-level transactions to avoid enhanced due diligence is a relevant transactional risk because repeated small deposits, withdrawals, or bets can be structured to evade internal thresholds, fragment the audit trail, and conceal the overall value and purpose of activity. Operators should aggregate linked activity across accounts, payment methods, and time periods rather than assessing transactions in isolation. FATF identifies non-face-to-face relationships and transactions as potentially higher-risk circumstances requiring enhanced measures where appropriate. See FATF Recommendations and the UK Gambling Commission's anti-money-laundering guidance.

QUESTION NO: 87

Money laundering can cause which consequences for a financial institution? (Select Two.)

A. Increases in corporate taxes

B. Increases in investigation costs and fines

C. Reduction in number of employees

D. Reduction or loss of profitable business

E. Increases in correspondent banking facilities

ANSWER: B D

Explanation:

"Increases in investigation costs and fines" is correct because a financial institution exposed to money laundering may need to spend substantial resources on internal investigations, transaction reviews, customer-file remediation, independent testing, legal counsel, and responses to regulatory or law-enforcement inquiries. Where anti-money laundering controls, suspicious activity reporting, or customer due-diligence measures are deficient, enforcement actions can also result in civil money penalties and other costly remedial obligations. "Reduction or loss of profitable business" is also correct because money-laundering allegations or enforcement actions can damage an institution's reputation and risk profile. Customers, investors, counterparties, and correspondent institutions may curtail, re-price, or terminate relationships, reducing revenue and limiting access to business opportunities. These effects demonstrate why an effective AML compliance program is a core financial and operational safeguard, not merely a regulatory requirement. FATF emphasizes that financial institutions must apply preventive AML/CFT measures, including customer due diligence and reporting of suspicious transactions, to protect the financial system from illicit-finance abuse. U.S. supervisory guidance likewise identifies the operational and enforcement significance of sound BSA/AML risk management. See the FATF Recommendations and the FFIEC BSA/AML Examination Manual.

QUESTION NO: 88

One area of responsibility for the Board of Directors when implementing a successful AML program is to:

A. ensure the appointment of a qualified chief AML officer.

B. create a culture of compliance based on the profit expectation.

C. manage the day-to-day processes of the compliance program.

D. hire a third-party firm to be responsible for the AML compliance.

ANSWER: A

Explanation:

Ensuring the appointment of a qualified chief AML officer is a core board-level responsibility because an effective AML program requires clearly accountable, competent leadership with sufficient authority, independence, and access to senior governance. The board establishes the program's governance framework and provides oversight; as part of that role, it must ensure that the person responsible for AML compliance has the expertise and organizational standing to administer the program, identify and escalate material AML risks, and report significant issues to senior management and the board. The designated officer's title can vary by institution and jurisdiction—for example, BSA Officer, AML Compliance Officer, or Money Laundering Reporting Officer—but the essential requirement is a qualified individual with responsibility for coordinating and maintaining the AML compliance function. Board oversight also supports this appointment by ensuring adequate resources, staffing, systems, and reporting lines for the officer to perform the role effectively. The FFIEC BSA/AML Examination Manual describes the board's responsibility to oversee the BSA/AML compliance program and designate a qualified individual responsible for coordinating and monitoring day-to-day compliance. FATF guidance likewise emphasizes governance, effective controls, and appropriate responsibility for AML/CFT compliance. See the FFIEC BSA/AML Examination Manual and the FATF Recommendations.

QUESTION NO: 89

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:

Certification of documents presented is correct because the Basel Committee identifies it as an example of a safeguard banks can use for customers who are not physically present during onboarding. Non-face-to-face relationships create a heightened identity-verification challenge: bank staff cannot inspect original identification in person, compare the document to the individual presenting it, or readily detect impersonation. Certification by an appropriate independent and reliable party provides additional assurance that identity evidence is authentic and has been checked against an original or otherwise validated source.

The Basel Committee’s customer due diligence guidance specifically states that banks should apply equally effective customer-identification procedures to non-face-to-face customers and lists certification of documents among the measures available to mitigate the increased risks. The control supports the CDD objective of establishing confidence in the customer’s identity before a relationship is accepted. Its risk-based application is also consistent with the FATF framework, which calls for specific and adequate measures to address the risks posed by non-face-to-face business relationships or transactions. See the Basel Committee’s Customer due diligence for banks and FATF Recommendations.

QUESTION NO: 90

Which risks inherent to real estate sector carry the highest AML/CFT risk? (Select Two.)

A. Use of cash to purchase property

B. Unlicensed real estate agents acting as front companies

C. Use of a registered trust for the purchase of property

D. Use of a company for the purchase of property

E. Manipulation of the value of a property

ANSWER: A E

Explanation:

Use of cash to purchase property and manipulation of the value of a property are particularly significant real-estate ML/TF vulnerabilities. A cash purchase can reduce the visibility created by lending institutions and can make it harder to establish the source of funds, identify the parties providing the funds, and detect unusual transaction patterns. Although cash transactions may be legitimate, they warrant heightened scrutiny when the customer’s known profile, source of wealth, or transaction rationale does not support the amount or manner of payment.

Manipulation of property value is also a well-established laundering technique. A property may be deliberately bought or sold at an inflated or deflated price, sometimes through related parties or repeated transactions, to transfer value, create an apparently legitimate explanation for illicit proceeds, or obscure the true economic purpose of the transaction. Reliable valuation information, a clear explanation for price deviations, and review of the parties’ relationship are therefore central controls. FATF identifies both large cash transactions and unusual pricing as relevant real-estate risk indicators and emphasizes risk-based due diligence and beneficial-ownership transparency in the sector. See the FATF report on concealment of beneficial ownership and the FATF report on money laundering through real estate.