PassQueen
a.k.a dumpsqueen.com

Advanced CAMS-Audit Certification Exam

ACAMS Advanced-CAMS-Audit

Version Demo

Total Demo Questions: 11

Total Premium Questions: 110

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An organization creates a document for its audit committee listing the outstanding audit findings. The list has an executive management owner assigned to each finding, due dates for reporting management's responses and space for management to identity the actions to be taken. Which is a primary purpose of this document?

A. Providing audit documentation of management responses

B. Tracking completion of proposed recommendations

C. Documenting audit team validation testing

D. Testing resiliency of proposed recommendations

ANSWER: B

Explanation:

Tracking completion of proposed recommendations is the primary purpose of this document because it creates a formal mechanism for governing and monitoring management's remediation of outstanding audit findings. Assigning an executive owner establishes clear accountability for each issue. Recording response deadlines and planned corrective actions enables the audit committee and internal audit function to monitor whether remediation is progressing as committed, whether overdue items require escalation, and whether material risks remain open.

Effective issue follow-up is a key part of audit governance. The audit committee needs concise, reliable reporting on unresolved findings, responsible parties, target dates, and remediation status so that it can exercise oversight of management's risk treatment. This type of tracker also supports a disciplined follow-up process: after management reports completion, internal audit can perform appropriate validation before a finding is formally closed. Thus, the document is principally a tool for tracking corrective-action completion and accountability, rather than merely retaining management's written responses.

The Institute of Internal Auditors describes the requirement to monitor the disposition of engagement results in its Global Internal Audit Standards. Additional audit-committee oversight guidance is available from the IIA guidance resources.

QUESTION NO: 2

Which products/services increase the risk level for money laundering for XYZ Bank?

A. Payable through accounts

B. International fund transfers

C. Letters of credit

D. Foreign exchange services

ANSWER: A B C D

Explanation:

Payable through accounts, international fund transfers, letters of credit, and foreign exchange services can each increase a bank's inherent money-laundering risk because they may involve cross-border activity, rapid movement or conversion of funds, multiple intermediaries, and reduced transparency regarding the parties underlying a transaction. Payable through accounts are particularly sensitive because a foreign correspondent's customers may access the account, requiring robust due diligence and monitoring by the respondent and correspondent institutions. International fund transfers can move value quickly across jurisdictions and through complex payment chains. Letters of credit are trade-finance instruments and require scrutiny of the transaction's commercial rationale, parties, goods, pricing, and documentation because trade-based money laundering can disguise illicit value transfers within apparently legitimate trade. Foreign exchange services permit conversion between currencies and may be used alongside cross-border transfers to obscure the origin, ownership, or destination of funds. The actual risk for XYZ Bank depends on factors such as customer type, countries involved, transaction volumes,

delivery channel, and the effectiveness of controls; however, each listed service is a recognized product area requiring risk-based AML controls. See the FFIEC BSA/AML Examination Manual and FATF's trade-based money laundering guidance.

QUESTION NO: 3

Which are methods to test internal controls related to the CDD and KYC process? (Select Two.)

A. Ask the account officers whether the CDD and KYC information provided is correct.

B. Confirm with client onboarding teams whether or not high-risk customers exist.

C. Review the accuracy of the gap analysis of the CDD and KYC policies and procedures against local regulations.

D. Evaluate the results of the sample testing of new and existing customer relationships for adherence to the CDD and KYC process.

E. Confirm if suspicious activity reports were filed following escalation for non-compliance with the CDD and KYC process.

ANSWER: C D

Explanation:

Reviewing the accuracy of the gap analysis of the CDD and KYC policies and procedures against local regulations is an appropriate control-testing method because it assesses whether the institution's documented framework is complete, current, and aligned with applicable legal and regulatory requirements. A meaningful gap analysis identifies discrepancies between the organization's policies, procedures, and control design and the requirements imposed by the jurisdictions in which it operates. This gives auditors evidence about whether controls have been designed to address customer identification, verification, beneficial ownership, risk classification, and ongoing monitoring obligations.

Evaluating the results of the sample testing of new and existing customer relationships for adherence to the CDD and KYC process is also essential because it tests operating effectiveness. By selecting files across customer types, risk levels, products, and relationship stages, the reviewer can determine whether staff consistently performed required due diligence, documented their rationale, obtained required approvals, and completed reviews or refreshes within required time frames. Together, policy-to-requirement gap analysis and transaction- or file-level sample testing provide evidence of both control design and implementation. The FATF's customer due diligence standard is available at FATF Recommendations, and practical examination guidance appears in the FFIEC Customer Due Diligence manual.

QUESTION NO: 4

Which are objectives of the issue confirmation step in the audit issue management process? (Select Two.)

A. Findings ate explained and assigned to the accountable owners.

B. Additional remediation is identified and planned.

C. Findings ate clearly written and facts are accurate

D. Communication, follow-up. and documentation are tracked on scheduled sustainability validations.

E. Compliance Identifies and schedules pre-exam validation as appropriate.

ANSWER: A C

Explanation:

The objectives of issue confirmation include ensuring that findings are communicated clearly, supported by accurate facts, and formally assigned to accountable owners. Clear articulation establishes a shared understanding of the condition, risk, criteria, and expected corrective action before remediation activity proceeds. Assigning ownership is essential because it creates accountability for developing and carrying out an appropriate management action plan.

Issue confirmation also requires that the finding be written clearly and that its factual basis be validated. Accurate, sufficiently supported documentation helps management acknowledge the issue, enables informed decisions about corrective action, and creates a reliable record for subsequent monitoring and closure. This aligns with internal-audit practice: audit communications should be accurate, objective, clear, concise, constructive, complete, and timely, while engagement results are communicated to appropriate parties. Effective issue management also depends on documented ownership and agreed actions that can later be monitored to completion. See the Institute of Internal Auditors' Global Internal Audit Standards and ACAMS' Advanced CAMS-Audit certification overview.

QUESTION NO: 5

Independent testing of the New York branch of a foreign bank is conducted by an outsourced audit firm. The independent testing report should be submitted to which authority in order to provide appropriate level of governance and oversight?

A. Main office risk management committee

B. Bank's designated board committee at the head office

C. Compliance oversight committee of the New York branch headed by the chief compliance officer

D. New York branch regulatory compliance committee headed by the chief incumbent of the branch

ANSWER: B

Explanation:

Bank's designated board committee at the head office is correct because independent testing is a key component of an effective Bank Secrecy Act/anti-money laundering compliance framework and requires escalation to an appropriately senior governing body. For a New York branch of a foreign bank, a designated board committee at the head office provides governance at the level of the institution responsible for establishing enterprise-wide compliance standards, allocating resources, challenging management, and ensuring that audit findings receive timely remediation. This reporting line also allows branch-specific findings to be assessed in the context of group-wide AML, sanctions, and regulatory risks.

New York's Transaction Monitoring and Filtering Program Regulation requires a covered institution's program to be subject to independent testing by internal audit or a qualified outside party. It further requires the resulting findings to be reported to the board of directors or a committee of the board, or to senior management, so that the institution has meaningful oversight and accountability. Where the foreign bank has designated a head-office board committee for this purpose, submitting the outsourced independent-testing report to that committee meets the expected board-level governance standard. See the New York DFS Part 504 regulation and the DFS's Part 504 guidance page.

QUESTION NO: 6

Which task should an auditor complete first when preparing to audit the client risk scoring methodology?

A. Query the completeness of the customer data to be provided.

B. Discuss the client risk scoring process with the head of AML.

C. Review the financial institution's AML risk assessment to understand the institution's client base.

D. Review a list of high-risk customers provided by compliance.

ANSWER: C

Explanation:

Review the financial institution's AML risk assessment to understand the institution's client base. is the appropriate first task because the enterprise-wide AML risk assessment establishes the context against which the client risk-scoring methodology should be designed, calibrated, and governed. It identifies the institution's relevant risk drivers, including customer types, products and services, geographies, delivery channels, and activity profiles, as well as the institution's risk appetite and mitigating controls. An auditor needs this foundational understanding before assessing whether customer-risk

factors, ratings, weighting, escalation criteria, and periodic-review requirements are reasonably aligned to the institution's actual AML exposure.

This review also enables the auditor to form a risk-based audit approach: testing can be directed toward client segments and circumstances that the institutional assessment identifies as materially higher risk. The methodology should produce customer classifications that support proportionate customer due diligence, enhanced due diligence where warranted, and effective ongoing monitoring. The FFIEC explains that a BSA/AML risk assessment is a critical component of developing a risk-focused program and evaluating risk exposure. FATF likewise requires institutions to identify and assess money-laundering and terrorist-financing risks and apply controls proportionate to those risks. See the FFIEC BSA/AML Examination Manual and FATF Recommendations.

QUESTION NO: 7

During a sanction review, an auditor notes that several of the bank's large corporate clients continue to route transactions through the bank to certain Office of Foreign AssetsControl (OFAC)-sanctioned countries.The head of corporate clients stated that these transactions were executed under the OFAC license.What should an auditor know to distinguish between an OFAC general license and a specific license?

A. A general license authorizes a type of transaction and a specific license authorizes a transaction in response to a written license application.

B. A specific license authorizes a transaction for an entity and a general license authorizes a transaction for an individual.

C. A general license authorizes a transaction for an entity and a specific license authorizes a transaction for an individual.

D. A specific license authorizes a type of transaction and a general license authorizes a transaction in response to a written license application.

ANSWER: A

Explanation:

A general license authorizes a type of transaction and a specific license authorizes a transaction in response to a written license application. OFAC issues general licenses by publishing them in the relevant sanctions regulations; they authorize categories of activity under stated terms and conditions and are available to any person whose proposed activity meets those conditions. A party ordinarily does not need to submit an application to OFAC to rely on an applicable general license, but it must ensure the transaction strictly satisfies all scope limitations, conditions, recordkeeping requirements, and any reporting obligations. In contrast, a specific license is a written authorization issued by OFAC in response to a license application. It permits the applicant to undertake the particular activity described in the license, subject to its express conditions, duration, parties, and transaction details. For audit purposes, the bank should therefore validate the applicable general-license provision or obtain and review the customer's specific-license documentation, confirm that it covers the relevant transaction, and retain evidence supporting the determination. OFAC describes these distinct authorization mechanisms in its Frequently Asked Question 221 and provides licensing guidance and application resources on its OFAC License Application Page.

QUESTION NO: 8

Which is considered a minimum requirement in a customer identification program?

A. Transaction reporting procedures used to report suspicious transactions to the regulator

B. Transaction monitoring procedures that specify the information that will be retained in each transaction

C. Account opening procedures that specify the information that will be obtained from each customer

D. Customer enhanced due diligence procedures used to identify unusual transactions

ANSWER: C

Explanation:

Account opening procedures that specify the information that will be obtained from each customer are a minimum requirement of a customer identification program (CIP). A CIP must be incorporated into the institution's anti-money laundering compliance program and must establish risk-based procedures for obtaining identifying information from each customer before an account is opened. At a minimum, for an individual, this information comprises the customer's name, date of birth, residential or business address, and an identification number. The institution must also establish procedures to verify the customer's identity within a reasonable time, maintain records of the information used to identify and verify the customer, and check the customer against applicable government lists. Clear account-opening procedures ensure these required data elements are gathered consistently at the point where the customer relationship begins, providing the basis for identity verification, customer due diligence, and subsequent risk assessment. The U.S. CIP rule is set out at 31 CFR § 1020.220. FATF's customer due diligence standard likewise requires financial institutions to identify customers and verify their identities using reliable, independent source documents, data, or information; see FATF Recommendation 10.

QUESTION NO: 9

Which scenarios should be used to monitor for potential elder abuse? (Select Two.)

A. Scenarios 1

B. Scenarios 2

C. Scenarios 5

D. Scenarios 7

E. Scenarios 8

ANSWER: D E

Explanation:

Scenarios 7 and 8 are appropriate for monitoring potential elder financial abuse because they focus on transactional activity that is anomalous when compared with an older customer's known financial profile and historical behavior. Effective monitoring for elder exploitation should identify sudden or unexplained large cash withdrawals, atypical wires or transfers, abrupt changes in spending or account use, and transactions that appear inconsistent with the customer's usual purpose, counterparties, or capacity. These patterns can indicate that a trusted person, caregiver, family member, or third party may be exerting undue influence or misusing access to the customer's funds. A risk-based monitoring program should use customer-profile information, account history, and available vulnerability indicators to generate alerts for timely review and escalation. The review should document the activity, assess whether there is a reasonable explanation, and determine whether a suspicious activity report is appropriate under the institution's procedures. FinCEN specifically identifies unusual account activity, including large or atypical withdrawals and transfers involving older adults, as a relevant financial-exploitation red flag. See FinCEN's advisory on reporting elder financial exploitation and the CFPB elder financial protection resources.

QUESTION NO: 10

An auditor identifies a significant backlog of transaction-monitoring alerts, including alerts that exceeded the institution's investigation time frames. Which corrective actions are most appropriate? (Select Two.)

A. Close all alerts older than the established investigation time frame.

B. Perform a documented, risk-based triage of the backlog and assign accountable owners and completion dates.

C. Conduct a lookback of delayed alerts and related activity to assess missed escalation or reporting decisions.

D. Increase scenario thresholds until alert volumes return to normal levels.

E. Stop generating new alerts until the existing backlog is cleared.

ANSWER: B C

Explanation:

A documented risk-based triage of the backlog is appropriate because it prioritizes alerts using factors such as customer risk, transaction value, geographic exposure, typology, and potential sanctions or terrorist-financing indicators. The institution should also perform a documented lookback of delayed alerts and related activity to determine whether suspicious activity was missed, whether additional investigation is required, and whether reporting obligations were affected.

Closing older alerts solely because of age would remove evidence without addressing risk. Increasing thresholds to reduce alert volume may conceal suspicious activity and should not be used as an immediate backlog-remediation measure without appropriate analysis and validation.

QUESTION NO: 11

Which finding must be first remediated in order to understand is risks the organization is exposed to?

A. Finding 1

B. Finding 3

C. Finding 5

D. Finding 8

ANSWER: A

Explanation:

Finding 1 should be remediated first because it concerns the foundational risk-assessment capability needed to identify and understand the organization's exposure to money laundering, terrorist financing, sanctions, fraud, and related financial-crime risks. A sound enterprise-wide risk assessment identifies relevant risk drivers—such as customers, products, delivery channels, geographies, transactions, and third-party relationships—and evaluates the inherent risk before determining whether controls reduce that exposure to an acceptable residual level. This baseline allows audit, compliance, and management to make risk-based decisions, prioritize control enhancements, and allocate investigative and monitoring resources appropriately.

Remediating the foundational assessment first also provides the information required to sequence subsequent remediation rationally. Once the organization has a current, documented view of its material risks and the effectiveness of existing controls, it can establish defensible priorities, owners, target dates, and testing criteria for the remaining findings. The FATF Risk-Based Approach requires institutions to identify, assess, and understand their ML/TF risks and to apply mitigation measures proportionate to those risks. Similarly, U.S. supervisory guidance describes a risk assessment as a key basis for developing and maintaining an appropriate BSA/AML compliance program. See the FATF Recommendations and the FFIEC BSA/AML Examination Manual.