

# ADVANCED CAMS-AUDIT



## Certify your Advanced Audit Expertise

Every organization needs to understand how their Anti-Financial Crime (AFC) program is performing. Effective auditing helps them do this.

Earning the Advanced CAMS-Audit certification demonstrates clear understanding of audit principles, and the judgment needed to evaluate financial crime risk controls and their effectiveness.

This is an advanced specialist level certification, designed for those conducting AFC audits, and others involved in the independent monitoring and testing of AFC controls.

### Advanced CAMS-Audit is now a global exam-based certification

Advanced CAMS-Audit is the certification that equips your mid-level and senior management workforce with the knowledge to reinforce internal controls, enhancing their ability to meet regulatory expectations. Formerly an in-person course, CAMS-Audit is now an exam-based program. Candidates can prepare for the exam at a convenient pace and take it virtually or in-person at selected locations.

What does Advanced CAMS-Audit cover?

**Corporate Governance and the Audit Function**

**Planning and Scoping an Audit**

**Fieldwork and Evaluation**

**Reporting, Management Actions, and Follow-ups**

### Who is Advanced CAMS-Audit for?

This qualification is ideally suited to:

- Internal Auditors
- External Auditors
- Supervisors of Audit Teams
- First Line Assurance Teams
- Second Line Compliance Monitoring and Testing teams, or Quality Assurance teams
- Teams preparing institutions for regulatory examination/inspections
- Teams performing bank examinations/inspections from a regulatory perspective
- Teams performing independent testing and assurance as part of special projects



## FAQ's

### Who is Eligible?

To apply, candidates must have previously passed the CAMS exam.

It is recommended that candidates have a minimum of five years of previous audit or audit-related experience.

### How to Get Certified



### Recertification

Advanced CAMS professionals are required to recertify every three years, to demonstrate continuing professional education.

This replaces your previous CAMS recertification process, and those holding more than one Advanced CAMS designation only recertify their most recent qualification.

## Certification Package and Pricing

For group discounts, [request a consultation](#).

#### The certification package includes:

- Study guide (PDF)
- Online study materials (review questions, post-assessment)
- Practice exam
- Certification exam

**Private sector:** US\$2,195

**Public sector:** US\$1,695

#### Add-On

#### Virtual Classroom Series (Add-On)

- Save up to US\$195 when bundled with the Certification Package!

US\$595

# CAMS-Audit Blueprint Statements

## A. Corporate Governance and the Audit Function (20%)

- A1.** Roles and responsibilities of the third line of defense (e.g. definition of assurance; conflicts of interest in audit; delineation between the third and second and first lines of defense/independent testing vs. quality assurance; relationship with regulators, management, and the Board of Directors; independence and aspects that can jeopardize independence)
- A2.** International bodies, organizations, and key documents related to AML audit (e.g. FATF, OFAC, FFIEC, European Directive on AML, UK JMLSG and Wolfsberg Principles on Risk Assessment/Sanctions Screening)
- A3.** AML program governance structure including, but not limited to, reporting lines, committees, training, oversight of outsourced functions in-house, to other departments (e.g. Client Onboarding), or to a third-party (e.g. a vendor performing sanctions screening on behalf of the institution)
- A4.** Factors that trigger an audit (e.g. mandated by legislation/regulator, cyclic, one-off, implementation of a new AML system/solution; new legislation; factors that trigger an audit vs. factors that trigger an assurance review)
- A5.** Stages of an AML audit process (e.g. preparation planning/scoping, fieldwork/testing, recommendations, reporting, and post-report tracking and validation)
- A6.** Differences and similarities between internal and external auditing (e.g. internal audit function vs. external audit firm, relationship between the external auditor and the institution, relationship between the internal auditor and external auditor)
- A7.** Types of audit approaches (e.g. risk-based, proportionate, continuous) and the execution of horizontal, vertical, thematic and project/program reviews
- A8.** Audit documentation process (e.g. documenting an audit work program/plan; identification of relevant stakeholders; specifying audit objectives; the risks and the mitigation)

- A9.** Emerging risks from new typologies (e.g. FinTech, cyber, cryptocurrency), new regulatory guidance/requirements, and new technologies/practices (e.g. artificial intelligence, machine learning)

- A10.** Computer Assisted Audit Technologies (CAATS; e.g. data warehouses, dashboards, management information systems (MIS))
- A11.** Continuous business monitoring as part of the third line of defense's assurance (e.g. regular discussions with Compliance on AML trends and horizon risks)

## B. Planning and Scoping (25%)

- B1.** Types of evidence supporting the testing strategy (e.g. policies, procedures, client profile documentation such as KYC/CDD/EDD), identification of which units to audit, the audit time-scope, and appropriate data gathering techniques during the audit (e.g. interviews, documentation, walkthroughs, process-maps, surveys)
- B2.** The role of policies and procedures in informing the audit plan
- B3.** Audit risk assessment, types of audit (e.g. Front Office, Compliance, IT (for systems, data), Operations, Change Management), risk assessment methodologies (top-down and bottom-up), and procedures associated with defining the scope
- B4.** Role of the AML risk assessment (i.e. as conducted by the second line) in informing audit planning and scoping (e.g. key audit considerations in AML risk assessment and evaluation of its effectiveness in assessing the risks and mitigating controls)
- B5.** Financial crime risks associated with different sectors/industries, products and services, policies and procedures, and customer types and how to assess them
- B6.** Components of AML risk mitigation (i.e. Identification & Verification Risk, Detection & Monitoring Risk, Compliance Risk, Regulatory/Prior Audit Risk)

**B7.** Types of sampling methodology (e.g. judgmental, risk-based, quantitative) and factors to consider when selecting a sample (e.g. size/nature of the population, number of newly-onboarded customers, PEPs, high-risk customers, degree of control, risk level)

**B8.** How to incorporate regulatory examination findings, provisions from enforcement actions, and other assessments (e.g. outcomes of past audits, results of consulting engagements, internal reports if conducting an external audit) from the monitoring/validation process

**B9.** Methodology used to determine the quantitative and qualitative dimensions of risk appetite, how metrics are monitored (e.g. KPI's and KRI's) against Board-approved risk appetite thresholds, and actions that can be taken to mitigate financial crime risk

**C. Fieldwork and Evaluation (40%)**

**C1.** Definition of design effectiveness and operating effectiveness

**C2.** How to evaluate the design of the AML risk assessment (e.g. methodology), and the results of the AML risk assessment

**C3.** How to evaluate the design effectiveness of AML program policies/procedures (i.e. gap analysis; currency and clarity of the policies/procedures)

**C4.** How to evaluate the operating effectiveness of each element of an AML program (e.g. CIP and KYC/EDD, SAR/STR/CTR processes, Sanctions screening, transaction monitoring, staff training, staff qualifications)

**C5.** How to assess the design and operating effectiveness of the customer risk rating methodology (e.g. whether customers are accurately identified and appropriately risk-rated)

**C6.** Controls governing AML programs (e.g. the characteristics of effective controls – the “who”, “what”, and “when”), and procedures for testing/assessing the design of a control and reviewing the results of a control tested during the audit scope period

**C7.** Elements of model risk management (MRM; e.g. screening systems model, transaction monitoring model, customer risk rating), regulatory expectations, their application to AML programs, and how to assess relevant models

**C8.** How to evaluate the design and development of AML systems and solutions (e.g. for transaction monitoring, name/transaction screening), including determinants/indicators of data quality and lineage (e.g. how to assess data at rest and in transit)

**C9.** Record-keeping (e.g. CDD records, transaction data and advices, and copies of traveler's checks, bank drafts, and cashier's checks) and record retention (e.g. what information needs to be captured by an institution and for how long it needs to be retained)

**C10.** The steps to a root cause analysis for issues identified, including repeat issues

**D. Reporting, Recommendations, and Follow-up (15%)**

**D1.** How to document the testing methodology and results in the audit work papers (e.g. how to ensure exceptions are properly identified, retaining supporting evidence for the audit planning and fieldwork)

**D2.** How to determine the level of risk of findings, including self-identified issues (i.e. low risk/medium risk/high risk; severity and likelihood) and distinguish between material and immaterial findings to make recommendations addressing root causes and the risk

**D3.** Communicating audit results (e.g. relevant stakeholders, what to communicate and when, elements of an audit report, how to conduct an exit/ close meeting)

**D4.** How to monitor the status of remedial actions, and ensure completion of the committed actions, including exception approval processes for extensions of target dates

**D5.** How to design and test a follow-up strategy to ensure closure of committed actions based on audit findings