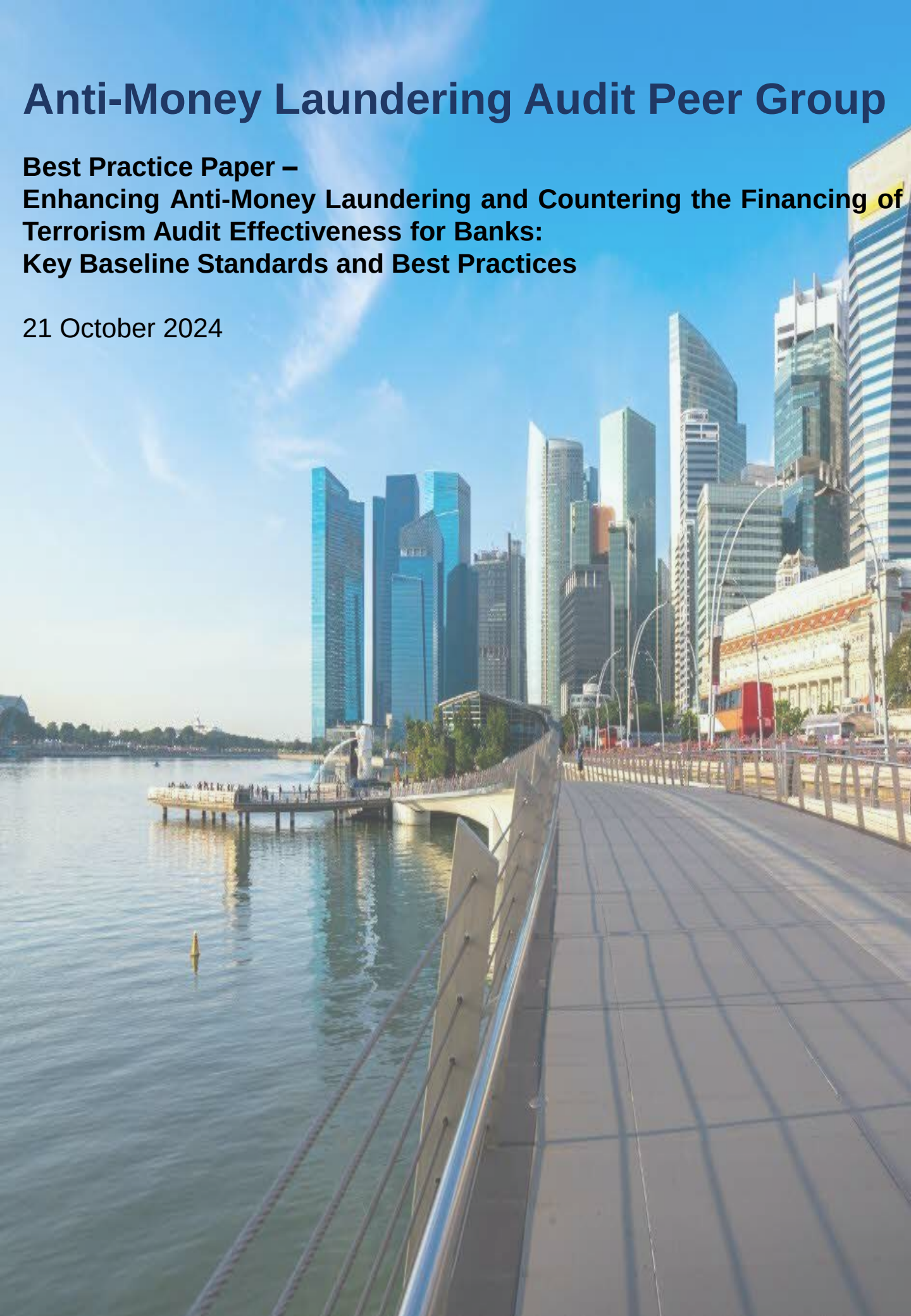
Anti-Money Laundering Audit Peer Group

Best Practice Paper –
Enhancing Anti-Money Laundering and Countering the Financing of Terrorism Audit Effectiveness for Banks:
Key Baseline Standards and Best Practices

21 October 2024



CONTENTS

CONTENTS

CONTENTS

Appendices

Annexes

1. Introduction

1.1 Background

Background

In October 2022, an industry-led **Anti-Money Laundering Audit Peer Group ("AAPG")** was established to (a) facilitate sharing of anti-money laundering and countering the financing of terrorism ("AML/CFT") audit best practices in the financial industry; and (b) promote engagement with the Monetary Authority of Singapore ("MAS") and the wider audit community on key AML/CFT risk areas. The establishment of the AAPG is in recognition that both the internal audit ("IA") functions and external audit ("EA") firms play key roles in ensuring that financial institutions' ("FIs") internal policies, procedures, and controls remain adequate to combat money laundering and terrorism financing ("ML/TF") and are in compliance with regulatory requirements.

AAPG Members

The AAPG is co-chaired by DBS Bank Ltd. ("DBS") and Oversea-Chinese Banking Corporation Limited ("OCBC") and comprises a wide-range of members from across the banking sector, professional services firms, and associations. The full list of members are:

Citibank Singapore Limited ("Citi");
Goldman Sachs (Singapore) Pte. ("GS");
GXS Bank Pte. Ltd. ("GXS");
HSBC Bank (Singapore) Limited ("HSBC");
MariBank Singapore Private Limited ("MariBank");
Standard Chartered Bank (Singapore) Limited ("SCB");
UBS AG Singapore Branch ("UBS");
United Overseas Bank Limited ("UOB");
BDO LLP ("BDO");
Deloitte and Touche LLP ("Deloitte");
Ernst and Young Advisory Pte. Ltd. ("EY");
Forvis Mazars LLP ("Mazars");
KPMG LLP ("KPMG");
PricewaterhouseCoopers LLP ("PwC");
The Institute of Internal Auditors ("IIA"), Singapore; and
The Institute of Singapore Chartered Accountants ("ISCA").

The MAS participates in the AAPG's discussions as an observer.

1.2 Objectives

Objective of the Paper

This paper aims to set out baseline standards and best practices for internal and external auditors to consider when determining the appropriate scope and extent of testing in the conduct of AML/CFT audits for banks.

This paper brings together the practices of AAPG members, as well as inputs from banks and audit firms that contributed to the AAPG's benchmarking survey in 2023. The survey solicited inputs on several aspects of audit practice, including:

- AML/CFT audit coverage;
- AML/CFT audit approach; and
- use of data analytics ("DA") and new techniques to strengthen AML/CFT audit effectiveness.

The results of the survey observed established baseline standards as well as surfaced several common focus areas for both internal and external auditors. In this paper, the AAPG has centered its detailed guidance on the following common focus areas:

Focus Area	IA	EA
Risk Assessment	✓	✓[1]
Scope and Methodology	✓	
Training and Upskilling	✓	✓
Reporting and Follow-up on Findings	✓	
Collaboration with Third Parties	✓	
Outsourced Anti-Money Laundering and Countering the Financing of Terrorism Functions	✓	
Partnering with Internal Audit		✓
Nature and Extent of Work to be Performed by External Audit Firms during Annual Audit		✓

[1] For external auditors, this includes how their risk assessment of the bank's business at the audit planning stage will determine the proposed scope of the audit.

1.2 Objectives

Objective of the Paper

In addition to the focus areas identified above, AAPG noted an increased adoption of DA and new techniques by internal and external auditors to strengthen AML/CFT audit effectiveness. Notably, DA has been used in the audit of business functions with AML/CFT responsibilities (such as those involved in customer due diligence ("CDD") and name screening) and has helped to more sharply identify higher risk customers/segments for closer audit scrutiny.

For the purposes of this paper, "Baseline Standards" and "Best Practices" have been defined as follows:

- ***Baseline Standards*** are expected minimum audit standards and practices that banks' IA functions and EA firms shall adopt and implement. Banks' IA functions and EA firms shall review their existing audit practices against the baseline standards, consider the areas that require enhancement to raise AML/CFT audit effectiveness, and formulate an implementation plan for these areas accordingly.

  – Non-adoption of baseline standards may be considered as having inadequate standards and practices, and considerations for non-adoption shall be well documented and endorsed by the Audit Committee.

  – Notwithstanding the baseline standards prescribed in this paper, banks' IA functions and EA firms shall also assess the need to include other AML/CFT coverage where relevant and/or appropriate.

- ***Best Practices*** are existing good practices identified from the administered survey, which can help to raise AML/CFT audit effectiveness. Banks' IA functions and EA firms are encouraged to adopt these best practices in commensuration with their banks'/clients' business and risk profiles.

All references to Audit Committee in this paper are to be construed as Audit Committee (if applicable) or for foreign bank branches with no local Audit Committee, senior management or regional/global Audit Committee.

This paper serves as a good starting point in providing the wider audit community with a common framework to support auditors' formulation of their views and assessment of banks' controls to mitigate ML/TF risks. While intended to provide guidance for the AML/CFT audit of banks, similar principles and practices set out in this paper may also be applicable in the AML/CFT audit of other FIs and sectors.

2. Internal Audit

2.1 Observed Baseline Standards

The following industry standards observed from the survey are key elements for ensuring the robustness of a bank's IA function and its audit effectiveness in relation to AML/CFT. These mainly relate to having (a) adequate governance and competency in the IA function; and (b) sufficient focus on AML/CFT on an ongoing basis.

(A) Adequate Governance and Competency in the IA Function

1 Governance and independence

- IA function shall report directly to the Audit Committee. Dual reporting (i.e., functional reporting to Audit Committee and administrative reporting to Chief Executive Officer/Country manager or equivalent) shall be established to ensure the independence of the IA function
- A formal IA charter shall be in place to establish “tone at the top” in support of the IA function

2 Operating model and team structure

- The regional IA function of a bank with a regional operating model may perform the audits of regional controls. The regional IA function shall have a good understanding of the nature of its bank's business and associated ML/TF risks

3 Skills, experiences, and knowledge

- Specific AML/CFT subject matter experts (“SMEs”) shall be identified within the IA function. These AML/CFT SMEs shall have knowledge on AML/CFT regulations and/or relevant AML/CFT working experience

2.1 Observed Baseline Standards

(B) Sufficient Focus on AML/CFT on an Ongoing Basis

1 AML/CFT audit framework

- IA function shall have an AML/CFT audit framework or audit strategy in place. Periodic review of such framework or strategy shall be performed at least annually with ad-hoc updates if there are:
  - material changes to the bank's business profile and strategy;
  - key changes driven by regulatory expectations or the bank's AML/CFT strategies;
  - key updates provided by IIA; and
  - material changes to the audit methodology.

2 Evaluation of documented AML/CFT policies, procedures, and controls

- IA function shall evaluate whether:
  - documented AML/CFT policies, procedures, and controls are adequate;
  - policies and procedures are regularly updated and clearly communicated throughout the bank;
  - controls implemented are stated in the policies and procedures;
  - requirements in the policies, procedures, and controls are reinforced through regular trainings; and
  - gaps identified, if any, are properly tracked, monitored, and resolved.

3 Audit focus areas and considerations for audit review

- AML/CFT is typically ranked within the top few audit focus areas, and audit resourcing and audit hours shall be commensurate with ML/TF related risk areas
- Considerations for AML/CFT audit shall include the bank's or business unit's susceptibility to ML/TF risks arising from business related factors (e.g., change in risk profile of target customer group, new businesses or products) or non-business related factors (e.g., change in operations or processes)

4 ML/TF risks or the business unit's susceptibility to ML/TF risks

- ML/TF risks, or the business unit's susceptibility to such risks, shall be a key consideration when identifying selected target areas for planning an audit. AML/CFT generally carries a higher risk rating for most auditable areas
- IA function shall consider conducting thematic AML/CFT audits to cover new and/or high growth business areas, among others, to ensure that front-line and ML/TF risk control functions remain effective given the increased ML/TF risks

5 Audit coverage to evaluate vulnerability of external business relationships ("EBRs")[2] to ML/TF risks

- During the audit engagement, depending on the scope and audit theme, the IA function shall evaluate:
  - if any EBRs are vulnerable to ML/TF risks; and
  - whether appropriate measures have been taken to adequately mitigate ML/TF risks and avoid reputational risks.

[2] EBRs include joint venture partners, outsourced service providers, agents, contract workers, vendors, franchisees, etc.

2.2 Focus Areas

To support a bank's IA function in its planning and execution of AML/CFT audits, this section sets out the baseline standards and best practices for six focus areas. Sample DA use cases from various banks are shared in Section 3.

1 *Risk Assessment*

This sub-section addresses some of the key factors to consider in an AML/CFT risk assessment to measure the inherent risks and control effectiveness.

2 *Scope and Methodology*

This sub-section addresses the scope and methodology for the provision of timely risk-based audit assurance on the AML/CFT control environment.

3 *Training and Upskilling*

This sub-section addresses the need for specific AML/CFT SMEs within the IA function, and regular tailored trainings covering areas such as emerging trends and regulatory needs.

4 *Reporting and Follow-up on Findings*

This sub-section covers the need to provide regular management reporting of material audit findings and addresses the expected follow-up actions.

5 *Collaboration with Third Parties*

This sub-section addresses how IA function can collaborate with Line 2 function and/or other internal assurance providers to optimize audit coverage and efficiency while continuing to be accountable for ensuring the quality of the third parties' AML/CFT risk management controls.

6 *Outsourced Anti-Money Laundering and Countering the Financing of Terrorism Functions*

This sub-section emphasizes the importance of ensuring similar focus and coverage for the audit of AML/CFT functions regardless of whether they are under outsourced arrangements.

Examples of DA:

This section provides examples of how a bank's IA function may use DA in conducting AML/CFT audits.

2.3 Focus Area 1: Risk Assessment

Outcome Statement

A bank's IA function shall have a good understanding of its bank's unique business model and ML/TF risks. In doing so, the IA function shall maintain an up-to-date AML/CFT audit universe and coverage plan that is commensurate with the risk profile of its bank, underpinned by robust risk assessment frameworks.

Baseline Standards

Various banks have their unique business models, each carrying its own set of inherent risks. It is essential to highlight that the baseline standards may not apply universally to all banks.

A bank's IA function shall conduct an AML/CFT risk assessment at least once a year to drive its audit plan. The bank shall customize its risk assessment according to its specific business model.

In doing so, a bank's IA function shall consider the following baseline areas to gauge inherent risks:

Categories	Baseline Areas

Customers	• Types of customers (e.g., corporates, individuals, private, public, FIs, and family offices)
	• Material changes in or new customer segments
	• Circumstances where a customer presents or may present a higher risk for ML/TF including where a customer:
	  • is from a higher inherent risk industry (e.g., money service business ("MSB"), virtual assets service provider ("VASP") business, and charity)
	  • is a politically exposed person ("PEP") or has adverse news
	  • has complex ownership structure and/or opaque ownership arrangement (e.g., partnership, joint venture, offshore company, trust, and shell company with no operations)

Products, Services, and Transactions	• Inherent ML/TF risks posed by the bank's products and services, especially in relation to:
	  • correspondent banking services
	  • trade finance facilities
	  • deposits, payments, local and cross border fund transfers or wire transfers
	  • nested accounts
	  • virtual assets including non-fungible tokens and cryptocurrencies
	• Material changes in or new products and/or services offered that may change the risk profile of the bank, including velocity of business changes (products and services)
	• Transaction profiles (e.g., pass-through profiles)

System Capability	• Material AML/CFT related system enhancement, integration, and migration • System resilience, including stability and management of cyber security risk that may arise from system issues impacting AML/CFT processes
Channels	• Extent of unsolicited business • Source of referrals (e.g., corporate service providers, external asset managers) • Extent of non-face-to-face channels

2.3 Focus Area 1: Risk Assessment

Categories	Baseline Areas
Geographies	• Customer's nationality, country of incorporation/birth/domicile, country of operations in high ML/TF risk jurisdictions***** • Beneficial owners from high ML/TF risk jurisdictions or who have transactions with high ML/TF risk jurisdictions • Customers possessing citizenship/residency through investment programs *****_As determined by banks based on global organizations or indexes including, but not limited to, the Financial Action Task Force's ("FATF") "black and grey" lists or lists obtained from reputable vendors' geographic risk rating methodology, as may be updated from time to time_
Mergers and Acquisitions	• AML/CFT risk impact arising from pre- and post- acquisition due diligence, gap analysis performed, issues identified etc. during mergers and acquisitions
AML/CFT Risk Landscape and Regulations	• AML/CFT risk landscape, including consideration of (a) recent ML/TF risk events (e.g., noted in the media); (b) ML/TF risk typologies or focus areas highlighted by the industry (e.g., via AML/CFT Industry Partnership ("ACIP")) and FATF; and (c) key ML/TF risk areas highlighted in the ML/TF national risk assessments of the jurisdictions that the bank operates in • Local laws, regulatory and legislative requirements, and upcoming changes. This shall include consideration of additional guidance issued by regulators via circulars and information papers • International regulatory requirements, where relevant

A bank's IA function shall consider the following baseline areas to gauge control effectiveness for residual risks:

Categories	Baseline Areas
Past Issues	• Number of overdue internal, external or regulatory issues, including enforcement actions • Number of recurring issues
Events	• Number and severity of risk events, incidents or near misses • Number of key risk indicator breaches (e.g., CDD backlogs, transaction monitoring ("TM") backlogs, delays in assessing suspicious transaction reports ("STRs"), and delays in taking risk mitigating measures post-suspicious transaction reporting) • Number/ratio of STR filings, sanctions breaches or regulatory breaches
Controls	• Review Line 1's self-assessments • Review Line 2's assurance reports and assessments • Review scope and results of EA or regulatory assessments • Review changes to controls or control processes • Review controls relating to Know Your Customer ("KYC")/CDD, customer risk assessment, onboarding, periodic reviews, ongoing monitoring, TM and name screening thresholds, and parameters being fit for purpose • Review governance and independent validation around artificial intelligence ("AI") and machine learning models (if any) • Review screening and watchlist operations • Review quality and timeliness of TM and name screening alerts disposition • Review quality and timeliness of investigations and STR filings • Review escalation and management oversight • Review evidence of rejecting customers with heightened risk that may be inconsistent with the bank's risk appetite, including escalation and aging of issues raised by Lines 1, 1.5, and 2.

2.3 Focus Area 1: Risk Assessment

Categories	Baseline Areas
Governance	• Review Line 2's oversight of activities and dispensations • Review approval process for new products or alterations and AML/CFT compliance's involvement for pre-implementation controls • Review reporting to senior management and board committees • Review evidence of follow-up actions on matters discussed at senior management forums and board committee meetings
Resources	• Adequacy of resources, especially in key ML/TF control functions and for business/customer segments that pose higher ML/TF risks • ML/TF risk awareness of Lines 1 and 2

Best Practices

Continuous Monitoring and Risk Assessment	Continuous monitoring and risk assessment are useful in facilitating detection or anticipation of emerging ML/TF risks in the dynamic business environment. The IA function's presence in governance and risk committees provide invaluable insights into the changing business requirements.
Usage of DA	Leverage DA to identify risk indicators, trends, and predictive indicators. Examples of DA that may be leveraged include: • using cluster analysis to gain insights into the customer population; and • using DA to complement the risk scoring model used by the bank for specific KYC areas such as source of wealth ("SOW") and source of funds ("SOF"). Further examples of DA are provided under Section 3.

2.4 Focus Area 2: Scope and Methodology

Outcome Statement

A bank's IA function shall perform regular AML/CFT audits, with a frequency and scope commensurate with the risk profile of its bank, having regard to the nature and complexity of its business. This shall cover areas of concern based on risk assessments performed, including relevant or evolving AML/CFT risks and typologies, and additional coverage of focus or risk areas as needed.

Baseline Standards

Scope*

- Develop an AML/CFT audit coverage strategy
- Cover all baseline areas within three years, or as required by the bank's risk assessment framework and as commensurate with the risk profile of the bank
- Conduct an audit of AML/CFT at least once a year covering higher risk areas
- Conduct periodic thematic AML/CFT reviews across various business lines or geographies for enhanced focus on higher risk or emerging areas, drawing reference from MAS 626 guidelines[3]
- Draw reference to the reviews done by EA firms and regulator during scoping to avoid duplication and to delve deeper into areas that may require greater management attention
- Consider the controls that have been outsourced under an outsourcing arrangement[4]

**Audits of the baseline areas may not be required if (i) the baseline areas have already been covered by an audit conducted by another entity within the group (e.g., Head Office); (ii) the extent of work performed by that entity addresses the regulatory requirements in Singapore; and (iii) samples are selected from the Singapore office for testing where relevant.*

For example, if the TM system is managed by Head Office and the coverage on calibration of the TM system is covered by the IA function in Head Office and samples from the Singapore office were included for testing where relevant, the Singapore office's IA function will not need to conduct a separate audit in this area.

Methodology

- Adopt sampling methodology that is:
  - representative of the population's risk attributes given the risks assessed; and
  - sufficient to support a reasonable conclusion.
- Apply a combination of outcome-based[5] and control effectiveness testing
- Exercise flexibility based on assessment of audit areas during planning and fieldwork
- Select methodology that best suits the specific purpose of the audit

Categories	Baseline Areas
Governance	• Governance structure that aligns with the set-up of the bank and is relevant to the audit entities ("AEs") or audit objectives • AML/CFT framework • Enterprise-wide risk assessment ("EWRA") for ML/TF risks • Board and senior management oversight, including communication/ reporting of AML/CFT related matters and escalation • Capacity, competency, and independence for discharge of duties • Roles and responsibilities are clearly defined • AML/CFT trainings

[3] https://www.mas.gov.sg/regulation/guidelines/guidelines-to-notice-626-on-prevention-of-money-laundering-and-cft-for-banks
[4] https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing
[5] Outcome-based testing focuses on the results or outcomes of a policy, program, or activity and aims to assess the effectiveness and efficiency in, and impact of, achieving its intended objectives and delivering value to its stakeholders

2.4 Focus Area 2: Scope and Methodology

Categories	Baseline Areas
Policies, Standards, and Guides	• Compliance with MAS 626[6] and equivalent • Significant regulatory changes
CDD	• Onboarding review • Periodic review • Trigger event review • Customer risk assessment process and methodology • Post STR review of existing customer relationship
Activity Surveillance/ Sanctions Screening	• Lists management on sanctions and non-sanctions lists • TM alerts assessment, scenarios, and calibration • Name screening/transaction screening assessment and calibration • Name screening and transaction pattern profiles • Data lineage[7]
Suspicious Transactions Reporting and Follow-up	• Reporting processes • Post-mortem review or lessons learned • Follow-up mechanism (CDD review, exit, and escalation)
AML Systems and Tools	• Application and general controls • Logical/algorithm controls of TM and screening systems • Parameters and thresholds settings for flagging potential ML/TF alerts • KYC or onboarding systems • Governance and performance of AI/machine learning models
Quality Assurance ("QA")	• Scope, effectiveness, and results reporting and resolution processes of QA team • Monitoring and testing processes

Best Practices

Usage of DA	Use DA in audit processes such as in function or population attributes profiling, sampling, and testing. **Governance** • Planning: Continuous risk assessment of AEs based on related key risk indicators, including but not limited to, number of overdue CDDs, high-risk customers, PEPs, STRs filed, sanctioned customers, and ML/TF related risk incidents

[6] https://www.mas.gov.sg/regulation/notices/notice-626

[7] Data lineage refers to the completeness and accuracy of data from the source system, including interface controls for accurate data ingestion.

2.4 Focus Area 2: Scope and Methodology

Best Practices

Usage of DA	**CDD** • Sampling: Identification of higher risk customers based on risk factors, including but not limited to, shell or front companies, transactions outliers, STRs filed, PEPs, country of domicile in a tax haven or high-risk country, and number of ML/TF risk related alerts • Testing (on-demand or continuous): Exception-based rules built to check on adherence to bank standards and guidance such as validating the accuracy of system calculated customer risk rating and completeness of KYC information (i.e., not blank or invalid format) • Network link analysis ("NLA"): Identification and analysis of hidden relationships between customers based on the following: common address, common contact information, common customer-to-customer relationship, common transaction originators or beneficiaries, and common ultimate beneficial owners **Activity Surveillance** • Sampling: Identification of potentially suspicious customers based on typologies such as round tripping, transactions with STR parties, and transactions to/from higher risk countries **Suspicious Transaction Reporting (including follow-up)** • Sampling: Identification of potentially suspicious customers based on STRs filed using supervised machine learning Further examples of DA are provided in Section 3.
Continuous Auditing	• Conduct continuous auditing of targeted areas for efficiency and larger population or period coverage (e.g., areas with higher assessed risk or high activity level/volume)
Guidance in Audit Manual	• Provide specific guidance for the planning and conducting of AML/CFT audits in the audit manual

2.5 Focus Area 3: Training and Upskilling

Outcome Statement

A bank's IA function shall have sufficiently skilled staff with relevant subject matter expertise to conduct effective and robust AML/CFT audits. The IA function shall identify specific AML/CFT SMEs within its team.

Baseline Standards

- A bank's IA function shall determine the required training hours for its staff and ensure regular trainings are conducted (at least once a year) with training records maintained
- Scope of trainings shall be tailored according to staff experience and skill sets, and include:
  - emerging trends and typologies in ML/TF
  - new/amended MAS and FATF requirements
  - specific product knowledge/industry players (e.g., cryptocurrencies and VASPs) where relevant
  - culture and control awareness such as identification of red flags including the follow up actions to be taken
- Training materials/methodology shall include:
  - case studies and examples for illustration
  - quiz to ascertain effectiveness of training

Best Practices

Professional Certifications[8]	Audit staff obtain certifications depending on the skillsets required for their area of audits to develop competencies in specialized domains such as financial crime, business, and information security. Examples of AML/CFT related certifications include: • Certified Anti Money Laundering Specialist ("CAMS") • Advanced CAMS – Audit Certification • International Compliance Association ("ICA") Diploma in Financial Crime Compliance (Singapore) • ICA Advanced Certificate in Regulatory & Financial Crime Compliance (Singapore) • Singapore University of Social Sciences – Certificate course on Financial Crime Compliance • Other relevant accredited programs for AML/CFT under the Institute of Banking and Finance Singapore's Standards Training Scheme ("IBF-STS")
Seminars	Audit staff attend knowledge sharing sessions among leading industry experts on: • emerging trends and typologies in ML/TF to identify areas of emerging risks; • new requirements from regulators or standard setting bodies; and • best practices or lessons learned within the industry or domain. Such sessions provide networking opportunities for future collaboration and access to expert opinion.
Continuous Learning	IA function fosters a culture that promotes continuous learning at all levels in its bank (e.g., sponsorship of professional certifications, and ensuring ease of access to relevant learning tools and resources to encourage learning).

[8] Refer to Appendix F for examples of IBF-STS accredited programs. Upon successful completion of eligible IBF-STS accredited program(s) and fulfillment of required number of Technical Skills and Competencies, individuals may apply for IBF Certification, subject to eligibility criteria being met.

2.5 Focus Area 3: Training and Upskilling

Best Practices

Training and Upskilling Programs	IA function implements internal training and upskilling programs such as: **1. Guest Auditor Program** • Allow staff from other business and support units to participate in audit engagements for a period between two weeks to six months, to gain understanding of the IA function and appreciation of ML/TF risks • Simultaneously, guest auditors provide the IA function with a different perspective on governance, risk management, and control from its business or support unit. Any potential conflicts of interest due to such deployment shall be carefully assessed and objectivity shall not be compromised
	2. Job Rotation • Allow staff to understand and experience different functions of the bank, acquire new skills and expand their network, through rotation for a period of between two weeks to three months
	3. Internal Mobility • Allow staff to transfer to other functions such as business, compliance, and other control functions which enables the IA function to expand its knowledge and business acumen

2.6 Focus Area 4: Reporting and Follow-up on Findings

Outcome Statement

A bank's IA function shall have access to and maintain a holistic view of findings and remediation actions from previous audits and regulatory inspections. This shall be taken into consideration as part of the IA function's assessment of its bank's control environment and scoping of its audit plan.

Baseline Standards

A. Reporting of IA, EA, and Regulatory Findings

- Periodic reporting to Audit Committee shall include significant risk exposures and control issues, governance issues, and other important matters
- Reporting on material issues instills accountability in post remediation monitoring and ensures effectiveness of the remedial measures. This prevents recurrence and facilitates the allocation of appropriate resources to address such issues

B. Follow-up on IA, EA, and Regulatory Findings

	IA Findings	Regulatory Findings*	EA Findings
To maintain objectivity, IA functions and EA firms shall remain independent from one another.			
Issue Validation	IA function shall define a consistent approach to evaluate: • remediation actions taken to address IA and regulatory findings. The action plans shall be monitored by means of a tracking system; and • material risk areas/issues highlighted by regulators as part of ongoing supervision of banks (if any).		An EA firm will validate the remediation actions taken to address EA findings. For further details on EA's coverage, please refer to the EA section commencing from Section 5 of this paper. *An EA firm may also be engaged by a bank (either on its own or at the request of MAS) to follow-up on regulatory findings.
Scope of Validation	Validation shall entail: • reviewing if controls designed are adequate to mitigate risks, including sustainability of the controls; and • performing testing on the operating effectiveness of the controls. Management plans shall be sustainable and address root causes to prevent recurrence.		
Extent and Timing of Testing	IA function shall consider limited or full testing depending on: • risk level of the findings; and • whether there are enough samples for meaningful testing. Post-validation substantive testing shall be done within a predefined time period of issue closure, or in the next audit.		
Post-validation	Outcomes that warrant attention shall be escalated to senior management and the Audit Committee (e.g., failed validations, and aged outstanding remediation). There shall be no obligation to close an issue if the management action is found to be inadequate during validation.		

2.6 Focus Area 4: Reporting and Follow-up on Findings

	IA Findings	Regulatory Findings	EA Findings
To maintain objectivity, IA functions and EA firms shall remain independent from one another.			
Coverage in the Next Audit	Findings (dependent on the risk rating) raised by the IA function and/or the regulator relevant to the AEs which have not been addressed or rectified by the AEs, or validated by the IA function by the next scheduled audit shall form part of the audit coverage for the next scheduled audit.		Findings (dependent on the risk rating) shall be considered for audit coverage for the next scheduled audit.

Best Practices

Reporting to Management and Audit Committee	• In addition to reporting of significant issues to the Audit Committee, provide thematic analysis based on issues across the three lines model which, although not currently material, may have the potential to be systemic due to changes in organizational strategies, changes in the regulatory landscape or evolving business risks • Report remediation status of all findings to the Audit Committee on a periodic basis

2.7 Focus Area 5: Collaboration with Third Parties

Outcome Statement

A bank's IA function shall be accountable and responsible if it decides to draw comfort from the audit work done by reliable third parties. Such collaboration with reliable third parties can be used to augment the IA function's expertise, optimize AML/CFT audit coverage and efficiency, and/or minimize duplication of coverage. It shall not compromise the objectivity and integrity of the IA function.

Baseline Standards

Key considerations for collaboration with third parties

A bank's IA function shall ensure that audit work performed by the third parties is reliable – for example, it shall not draw comfort from audit work performed by Line 1 on itself.

A bank's IA function shall not solely depend on the audit work done by reliable third parties to cover the baseline audit areas for AML/CFT as specified in "2.4 Focus Area 2: Scope and Methodology". The IA function shall be involved in covering the baseline audit areas for AML/CFT unless additional expertise is needed or there is a need to optimize the AML/CFT audit coverage and efficiency.

Where a bank's IA function decides to draw comfort from the audit work of third parties, it shall assess the following:

- Areas and extent of reliance;
- Reliability and adequacy of the work done by third parties;
- Relevance and validity of professional experience, qualifications, and certifications;
- Methodology, due professional care, and independence in planning, supervising, documenting, and reviewing the work;
- Whether third parties are clear in purpose and committed to providing assurance on a specified risk area and their work is relevant to the IA function's objectives and scope;
- Whether the work of third parties is performed and supervised in accordance with quality standards;
- Whether third parties are knowledgeable about the bank's risks, controls and what constitutes a weakness or deficiency;
- Potential or actual conflicts of interest and whether disclosures were made;
- Reporting relationships and the potential impacts of this arrangement; and
- Findings and conclusions and whether they are reasonable, and based on sufficient, reliable, and relevant evidence.

Notwithstanding the audit coverage by reliable third parties, a bank's IA function shall ensure audit coverage in areas with material ML/TF risk concerns that warrant stronger independent assurance to ascertain the robustness of controls.

There shall be engagement of the bank's Audit Committee to ensure that they are agreeable to and clear on the areas and extent of reliance, and adequacy of coverage.

2.7.1 Illustrative Example 1

The bank's audit methodology enables its IA function to draw comfort from reliable third party's (generally, Line 2) oversight of controls.

Background

The bank's audit methodology enables its IA function to draw comfort from Line 2's oversight of controls, such as ongoing monitoring by a reliable risk manager and the assurance work done by Line 2. To effectively draw comfort from these third-party activities, the IA function exercises informed judgment regarding their reliability and assess the extent to which it can draw comfort from their work.

Key Points to Note

Assessment	The IA function objectively assesses the maturity of the relevant third party's oversight framework as well as the quality and coverage of its work in managing the bank's overall ML/TF risks.
Activities Performed by Third Party	The IA function draws comfort from third-party testing and applies a reduced sample size for independent testing if its assessment is that the third party is reliable and effectively demonstrates the adequacy and effectiveness of the third party's oversight of the underlying business control(s). However, if the IA function's assessment is that the third party cannot demonstrate adequate oversight of the underlying business control(s), it will conduct independent testing without any reduction in the sample size. Prior to drawing comfort from such third party's oversight activities, the IA function: • considers the third party's review or assurance methodology, policies and procedures, including periodic review plans, resource skill sets, continuous professional development, quality improvement program, objectivity, and level of independence; • evaluates the extent of the third party's specific review and objectives, including competencies in terms of experience, qualifications, and skills; • reviews the outcomes of the third party's work and findings supported by their review documentation; and • assesses any supplementary work that may be required.

2.8 Focus Area 6: Outsourced Anti-Money Laundering and Countering the Financing of Terrorism Functions

Outcome Statement

A bank's IA function shall accord similar focus and rigor of coverage for both in-house and outsourced AML/CFT functions.

Baseline Standards

- A bank's IA function shall:
  - include AML/CFT functions under outsourced arrangements in the AML/CFT risk assessment, along with other AML/CFT functions within the bank, during the planning phase and while determining the focus and frequency of the audit
  - audit compliance of the AML/CFT functions under outsourced arrangements against MAS' requirements relating to outsourcing, including:
    - whether the controls implemented are adequate and commensurate with the nature and extent of risks arising from outsourced services;
    - whether key controls such as QA, oversight and monitoring of the established key risk indicators and contractual obligations are in place; and
    - whether a right to audit clause was included in the outsourcing arrangements.
  - ensure that the audit approach and coverage for in-house and outsourced AML/CFT functions are similar. Audit sample size shall be commensurate with the nature and extent of services provided under the outsourced arrangements
  - provide clear justification for the differences in scope and methodology for intra-group outsourcing functions (if any)
  - consider the requirements or controls of the host country in the audit coverage

- Should the bank's IA function be outsourced, the entity to which the function is outsourced is required to adhere to the baseline standards set forth in this paper

Best Practices

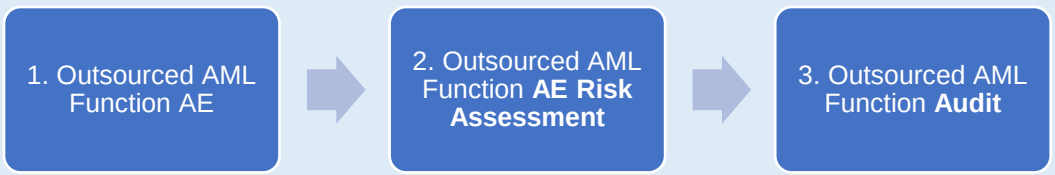
Audits on Outsourcing	Where a separate audit is conducted for compliance with MAS' requirements relating to outsourcing, such coverage is considered while performing AML/CFT audit of the functions under outsourced arrangements to avoid duplication of efforts. Periodic onsite audits are encouraged where outsourced operations are outside of the bank's premises.
Operational Risks	Other operational risks that directly impact the AML/CFT functions are considered as part of the AML/CFT audit coverage.

2.8.1 Illustrative Example 2

As part of the bank's audit universe, the bank maintains a list of AEs performing AML/CFT functions, including critical third parties, and both internal and external providers of goods and services. This list captures the scope and activities of each outsourced function (the "service provider").

Background

The bank maintains a list of the AEs performing AML/CFT functions, including critical third parties, and both internal and external providers of goods or services, as part of the bank's audit universe. This list captures the scope and activities of each service provider. The AEs of each service provider (hereinafter referred to as "hubs"') will be subject to regular business monitoring to inform of any changes to each AE's risk assessment which will, in turn, drive the audit coverage.



Examples of such outsourced functions include KYC operations hubs, AML TM hubs, and sanctions screening operations hubs.

Key Points to Note

AE Risk Assessment	AEs are subject to regular risk assessments. The risk assessment needs to consider overall inherent risk of the business activities, including: • risks arising from activities and processes carried out by the hub, such as operational risks, regulatory compliance risks, ML/TF risks, sanctions risks, information security risks, and technology risks; • volume and severity of prior or outstanding issues, such as issues that are self-identified, or raised by the bank's IA function, regulators or other third parties, to assess the control environment; and • control assessment considering top-down thematic risks, senior management and board committee's inputs, emerging risks, as well as culture and conduct factors for in-house and outsourced activities, in order to derive the residual risk of the outsourced function. Risk assessments must be dynamic, with updates throughout the year to reflect changes to internal controls, infrastructure, processes, business lines or laws and regulations. Assessments must also consider thematic control issues, risk tolerance limits, and conclusions on the effectiveness of governance.
Audit Coverage and Methodology	The AE risk assessment drives the audit frequency and coverage requirements. Audit coverage typically comprises of AML/CFT processes and controls owned by both in-house and outsourced service providers. The IA methodology focuses on key processes relating to a business or function and related risk to decide on audit requirements and scope, irrespective of the type of service provider (i.e., in-house and outsourced).

2.8.1 Illustrative Example 2

Key Points to Note

Audit Scope

The risk assessment drives scoping considerations and focus on areas of higher risks during the audits of the hubs. Audit coverage typically comprises of the processes and controls owned by the hub such as:

- execution of the bank's outsourced processes and controls;
    - For example, when auditing a TM hub, the audit will cover controls associated with the outsourced alert review and disposition and the end-to-end process executed by the hub
- governance and oversight over adherence to service level agreements and agreed upon procedures with the bank, such as delivery or completion timelines; compliance to bank's regulatory requirements or country variances; management reporting obligations to the bank; and
    - For example, service level, policy or regulatory breaches, key matters for attention, or key performance indicators
- other key controls owned by the hub in mitigating material risks identified in the risk assessment.
    - For example, information security associated with handling sensitive customer information, capacity in handling volumes, system and application controls, staff training and qualification etc.

In addition, the IA function will consider the adequacy of sample size representative of the bank or respective service recipients supported by the hub.

3. Data Analytics

3.1 Uses of Data Analytics

The increased adoption of DA by internal auditors has helped to strengthen AML/CFT audit effectiveness. Use cases of DA in IA functions include (a) automating processes to better quantify and draw out potential risk areas and anomalies across the bank; (b) providing an overview of essential business information by systematically and efficiently utilizing gathered data or through data mining; and (c) supporting more targeted audits by focusing on risk themes and/or identifying higher risk cases for attention. In a dynamic business environment, it is important for banks' IA functions to continually harness the power of DA in their audits.

This section provides examples of how banks' IA functions have used DA to support the audit of AML/CFT controls and processes.

3.2 Types of Data Analytics

- **Descriptive analysis**: Seeks information and applies hindsight to identify "What happened?"
- **Diagnostic analysis**: Applies hindsight and examines specific reasons "Why did this happen?"
- **Predictive analysis**: Applies insight to transform data into information to determine the probability of an event recurrence "What or when will it happen?"
- **Prescriptive analysis**: Utilizes foresight and scenario analysis to determine the course of action that would lead to potential outcomes "What should be done?"

3.3 Examples of Data Analytics in Internal Audit Functions

Example 1: The bank's IA function focuses on high-risk customer analytics to highlight customers with higher risk attributes for AML/CFT audit sampling using customer and transaction data.

Background

DA was developed to provide a standardized and consistent method to efficiently identify customers with higher risk attributes that may be applied across multiple AML/CFT related audits within and outside of Singapore.

The tool leverages a risk scoring approach based on in-house developed high-risk indicators, comprising the following "risk pillars":

1. High-risk KYC profile (e.g., cash-intensive businesses, and high-risk industries that are susceptible to ML/TF risks)
2. High-risk transaction indicators (e.g., potential pass-through transaction behavior based on aggregate transactions within a timeframe, and transaction with "high-risk" countries)
3. High-risk AML/CFT red flags based on known AML/CFT typologies. Examples include:
    - use of network analysis to identify customers with common addresses based on registered address records;
    - identification of "highly connected" beneficial owners associated with a high number of entities, and identification of these entities;
    - identification of counterparties of customers with potential virtual assets nexus based on counterparty names (e.g., keywords such as wallet, and coin); and
    - identification of individual customers with differences in nationality and birth country in the records, and where the nationality is a country that offers a "golden passport".

How did data analytics help in the audit process?

Systematic and Risk-based Methodology	DA deployed on both customer and transaction data enabled a systematic and risk-based method for the bank's IA function to select samples of customers for an in-depth review during audits.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 2: The bank's IA function uses a combination of a customer risk scoring model and keyword searches to identify samples for CDD review during its audit process.

Background

A DA tool was used to develop a risk scoring model to arrive at a risk score for each business relationship. The risk scoring model includes the following criteria with thresholds applied:

1. amount of assets under management;
2. the nature of the customer risk indicators as assessed under the bank's AML/CFT framework (e.g., PEPs, high AML risk business activities, high-risk jurisdictions as defined by industry practice and/or not in line with the bank's risk appetite ("high-risk jurisdictions"), fiduciary structures, complex structures, fiscal risks, and enhanced monitoring (negative news or STRs filed));
3. domicile or nationality in a country known as a typical tax haven or offshore location;
4. incoming or outgoing payments to/from a country without tax obligation;
5. incoming or outgoing payments to/from a high-risk jurisdiction;
6. account turnover (i.e., turnover of funds in the account);
7. proportion of flow-through transactions; and
8. number of ML/TF risk related alerts (i.e., number of TM alerts, including both true and false positives triggered on the account).

Given the total scores, the bank's IA function selected the samples (customer or common beneficial owner with a group of accounts) based on the following:

1. highest risk score based on the model;
2. customers representing different market desks (geographic locations) or serviced by different front office staff; and
3. customers representing different risk sensitivities per defined risk indicators.

In addition, the bank's IA function performed keyword searches to identify additional samples with specific risk themes (e.g., bitcoin, crowdfunding, and gift). This was used to complement the risk scoring model and identify additional samples of concern that may not have been identified by the model.

How did data analytics help in the audit process?

Targeted Sample Selection	A risk scoring model is used to identify and prioritize customers with high-risk scores for sample selection. Keyword filtering is applied to capture quantitative and qualitative characteristics/attributes of the customer populations. During the fieldwork phase, DA results are examined to identify concentrations and outliers from any criterion (e.g., account turnover, and proportion of flow-through transactions) within the risk scoring model.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 3: The bank's IA function uses (a) time series analysis and (b) cluster analysis to focus on sampling of high-risk areas.

Background

a) Time series analysis – Operational risk analysis

The bank's IA function independently obtains and analyzes the bank's data on operational risk events during the audit period to identify changes, trends, and patterns to inform its decisions on the areas of focus and sampling approach for the audited function. The bank has in place bank-specific reportable criteria/threshold for operational risk events based on both financial and non-financial factors. This may assist the bank's IA function in determining the focus areas through continuous monitoring (e.g., remediation tracking) or audits (e.g., validation of the remediation implemented). Examples of potential relevant operational risk events include:

- Technology: data integrity or change management issues which inadvertently impact TM or surveillance, negative news screening controls with potential regulatory impact;
- Process: lapses in manual processes that have a regulatory impact, such as the omission of specific AML/CFT related steps (e.g., local versus headquarters/global requirements), compliance with record-keeping/maintenance requirements, and lapses in outsourcing practices; and
- Regulatory responses: receipt of private warnings/reprimands and public enforcement actions.

b) Cluster analysis – Risk-based sampling for customer onboarding

The bank's IA function performs customer profile segmentation by sorting multiple data attributes obtained from customer profiles into smaller homogeneous clusters/segments to gain insights into a large customer population to facilitate targeted sample selection for audit testing.

By grouping customers with the same attributes together, the bank's IA function can better understand the different characteristics that define the customer population. A basic segmentation may consider customer domicile jurisdiction, customer type, customer citizenship(s), sales coverage representative, wealth, and years of engagement with the bank.

The bank's IA function is more targeted in its audit sampling through focusing on customers that reflect higher risk attributes and increasing the number of samples selected.

How did data analytics help in the audit process?

Targeted Sample Selection	The DA tools above enable the IA function to: • improve the efficiency and effectiveness of its audits; and • focus on higher risk areas and cover the audit population more meaningfully.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 4: The bank's IA function uses computer-assisted audit techniques ("CAATs") to identify anomalies in CDD and name screening, and thereby improving audit quality.

Background

The bank's IA function used CAATs to:

- detect potential deviation of KYC profiles that do not meet the bank's KYC standards and/or local regulations;
- identify customers (individuals or legal persons) with blank SOW;
- identify customers assessed to be of higher ML/TF risks, with low or no SOW corroboration;
- identify customers with inadequate SOW corroboration with reference to the strength of documents or information source as defined in the policy;
- identify customers with an overridden customer risk framework ("CRF") rating without an adequate and appropriate rationale;
- identify new account holders during audit period without approved product usage profiles ("PUP"); and
- identify exceptions where name screening alerts were not resolved or disposed properly within the established timeline as defined in the policies and procedures.

How did data analytics help in the audit process?

Detect Material Anomaly	The DA tool assisted the bank's IA function in: • automating the detection of potential exceptions for auditing KYC and CDD processes; • identifying newly onboarded customers, both individuals and legal persons, with no documented SOW corroboration and performing further investigation of the rationale for the omission of such documentation; • identifying anomalies in customers assessed to be of higher ML/TF risks but have low or no SOW corroboration and performing further investigation to understand the reason for the observed strength of SOW corroboration; • identifying inconsistencies between customer risk rating and strength of SOW corroboration. This helped to highlight customer relationships that fell outside of the bank's risk appetite and were non-compliant with regulatory requirements; • identifying test samples where CRF ratings were overridden to a lower risk rating and performing investigation to ascertain the adequacy and appropriateness of the rationale provided; • identifying anomalies whereby the PUP form was not completed for newly approved accounts and performing investigation to understand the rationale for the incomplete forms prior to approving new customer accounts; and • identifying anomalies in name screening alerts, which were not resolved or disposed properly within the timeline as required by the bank's policies and procedures, and performing investigation to identify genuine exceptions of late clearance of name screening alerts.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 5: The bank's IA function uses natural language processing ("NLP") or machine learning techniques and text mining or automated testing tool to assist with the audit of disposition of TM and name screening alerts.

Background

The bank's IA function leverages DA to assist its audit in the following areas:

A) TM Alerts Disposition

- As part of the IA function's testing of the TM control, case disposition templates ("CDTs"), which contain details of analysts' investigation and disposition of automated ML/TF risk related TM alerts, are sampled by the IA function to assess if they have been adequately reviewed at Level 1, escalated to Level 2 for investigation and where needed, further filed as STRs
- A high volume of automated alerts is generated for review, with the majority closed as false positives. Furthermore, each CDT may contain large number of texts (3,000 words or above) to support the disposition of each alerted case
- The IA function developed the DA model to efficiently search the entire population of cases and texts within each CDT by applying machine learning techniques to previously reported suspicious cases

B) Customer Screening Alerts Disposition

- The DA tool was developed to provide an automated means of detecting potential anomalies, reducing the need for manual IA checks in screening alerts escalated for Level 2 review. It leverages text mining and automated testing tools for Level 2 customer screening alerts
- Text mining is conducted on the analyst's notes and disposition comments to identify whether words related to high-risk areas are mentioned (e.g., references to high-risk countries and cryptocurrency related terms)
- Data mining is used to highlight potential anomalies, such as long-aging alerts and alerts that do not meet minimum review requirements

How did data analytics help in the audit process?

Detect Material Anomaly	The use of DA tools enables the bank's IA function to focus its resources on potential exceptions and higher risk samples. • The IA function leveraged NLP or machine learning frameworks to develop models that can extract and process large volumes of CDTs. The model has been trained to identify verbiage or semantics to automatically identify potentially incorrect case dispositions. This enables the IA function to focus manual judgment review efforts on potential exceptions • The tool assists the IA function in focusing on alerts that contain keyword mentions of interest and detect alerts that may lack rigor in their review, allowing the IA function to focus manual judgment review efforts on higher risk samples

3.3 Examples of Data Analytics in Internal Audit Functions

Example 6: The bank's IA function uses unsupervised TM scoring machine learning model to identify potential TM alerts that had not been properly assessed by TM analysts.

Background

An in-house risk scoring machine learning model was developed to identify potential outliers of TM alerts assessments.

The algorithm's primary function is to identify anomalies through a multivariate approach without any prior knowledge (i.e., it constructs the isolation forest based solely on the distribution of features identified within the transactions). Some of these features include customer information, unusual transaction records, exit registers, risk ratings of customers, and transactional data.

The transaction risk scores facilitated the IA function to perform targeted audit sampling on TM alerts that may not have been properly assessed by TM analysts, allowing for the prioritization of follow-up on alerts with higher transaction risk scores.

How did data analytics help in the audit process? 👍

Targeted Audit Sampling	The model's risk scores facilitated the identification of targeted samples for outcome-based assessment of the effectiveness of TM analysts.

3.3 Examples of Data Analytics in Internal Audit Functions

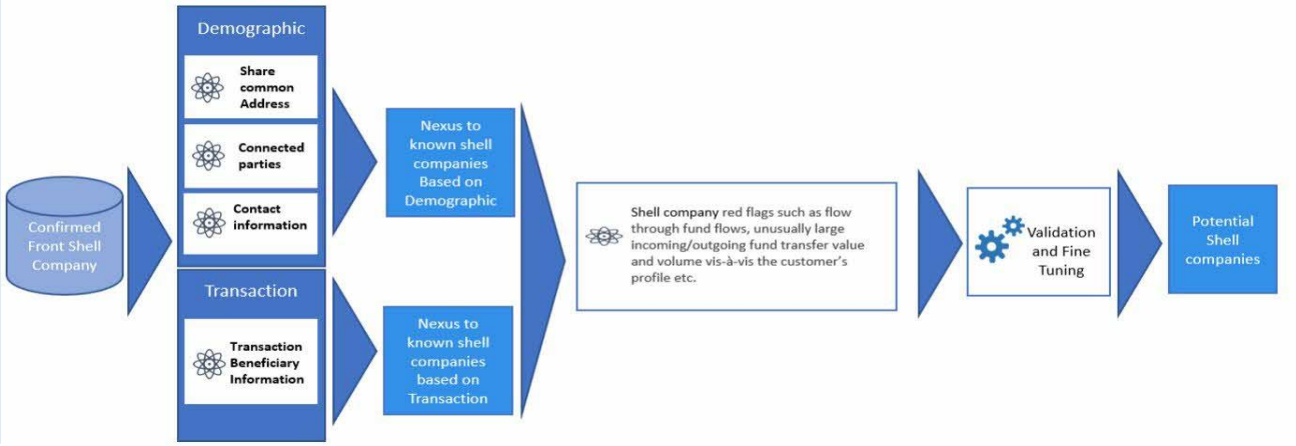
Example 7: The bank's IA function uses NLA to identify potential shell companies by detecting hidden clusters and recognizing characteristics typical of shell companies.

Background

The bank's IA function uses NLA to identify potential shell companies that may not be detected by existing controls. This strengthens its capabilities in assessing the adequacy and effectiveness of existing control measures for identifying shell companies.

NLA is used to:

- detect hidden clusters of shell companies by identifying entities sharing common related parties with abnormal transaction behavior in terms of volume and value; and
- identify customers with nexus (relationship or transactional) to known shell companies that are exhibiting characteristics typical of shell companies.



How did data analytics help in the audit process?

Identify Potential Shell Companies	The use of DA has sharpened the IA function's sampling process and detection capabilities to identify potential shell companies.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 8: The bank's IA function uses fuzzy logic name matching to identify potential inaccurate name screening alerts assessments.

Background

A fuzzy logic name matching tool was developed to identify name screening alerts inaccurately assessed as false hits due to full name mismatch.

The fuzzy logic name matching tool automatically highlights similar names (with higher scores), which have been assessed as false hits based solely on name spelling differences. The potential exceptions generated by the matching tool are reviewed as part of the audit testing on the operating effectiveness of the alerts assessments.

How did data analytics help in the audit process? 👍

Detect Errors in Name Screening Alerts	The use of DA facilitated a broader coverage in the assessment of name screening alerts, which are substantial in volume, with a targeted focus on potential dispositions inaccurately assessed as full name mismatch.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 9: The bank's IA function uses automated audit testing to detect (electronic banking) user setup containing numbers, symbols or initials.

Background

Where user setup is performed directly by customers via secure access gateways, errors in the registration of names submitted by customers are not always identified timely, potentially leading to ineffective screening of usernames.

The bank's IA function used automated audit testing to identify commercial card holders that had registered their names in a non-standardized format (e.g., containing numbers, symbols or initials), which prevented the detection of positive name matches during name screening and thus impacted the accuracy of AML/CFT name screening results.

Full population testing on a real time basis enables timely identification of exceptions.

How did data analytics help in the audit process?

Detect Material Anomaly	The use of DA has provided an automated mechanism for faster and wider (i.e., a large population) detection of exceptions in the registered names that are subjected to screening. Improved analytics, potentially conducted in real time, can be handed over to the business (Line 1) with the IA function performing audit testing on the actions taken by the business for the exceptions identified.

3.3 Examples of Data Analytics in Internal Audit Functions

Example 10: The bank's IA function employs a multifaceted approach that combines rule-based analytics, supervised machine learning, and data visualization to identify customers and related entities posing higher ML/TF risks across business segments.

Background

An AML/CFT audit DA tool was developed to conduct risk-based auditing effectively across three key ML/TF risk control processes:

1. KYC/CDD
2. Activity surveillance
3. STR reporting and follow-up

By leveraging customers' static data, transactions and STR records, the tool employs a combination of rule-based analytics and supervised machine learning model to examine various ML/TF risk typologies, identify suspicious patterns, and assign risk scores to each customer. This risk scoring enables the IA function to prioritize its review efforts on higher risk areas.

Rule-based analytics involves clustering customers into different risk typologies based on their transactional behaviors and profiles. Risk typologies include circular fund flow between parties (i.e., round tripping), and transactions with higher risk parties (e.g., parties with STRs filed against them, MSBs, parties associated with higher risk jurisdictions, and companies exhibiting attributes typical of shell companies).

The AML/CFT audit DA tool also incorporates relevant risk indicators as features into a supervised machine learning model. By training the model using STR cases as labels, the model assigns a risk score to each customer based on the customer's transactions. Customers are ranked based on their scores for the purpose of sample selection, with an explainer to indicate the top five features that contributed most to the customer risk score. This assists the IA function in identifying targeted samples and homing in on the area of focus.

To facilitate continuous monitoring, selected risk indicators from this tool are used in the bank's regular risk assessments. This enables the early identification of potential risk hotspots, allowing for prompt actions to be taken.

How did data analytics help in the audit process? 👍

Detect Material Anomaly	The tool improved the effectiveness and efficiency of audit sampling for deep dives, especially for common customers/relationships across different business segments. The tool enables the IA function to view the common relationships across business segments more easily and perform more holistic reviews to assess the consistency of the CDD risk assessments performed and risk ratings assigned across the different business segments. Given the large customer database and transaction volume, the tool also enables the IA function to prioritize the review of customers with higher risk scores across the different business segments.

4. Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases

Background

MAS jointly developed a digital platform, Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases ("COSMIC"), with six major commercial banks in Singapore, namely DBS, OCBC, UOB, SCB, Citi, and HSBC ("participating FIs").

COSMIC enables secure sharing of customer risk information among participating FIs to better detect ML, TF, and proliferation financing ("PF") risks, and support participating FIs in making more informed risk assessments.

The sharing of risk information is permitted only if the behaviors and transaction activities of relevant parties, including customers, exhibit multiple red flags that cross certain risk thresholds, suggesting that potential financial crime could be taking place.

COSMIC was launched on 1 April 2024. Risk information sharing is voluntary in the initial phase, which focuses on the following three key financial crime risks:

- misuse of legal persons;
- misuse of trade finance for illicit purposes, and
- PF.

MAS will consider expanding the number of participating FIs and the key risk areas.

Participating FIs are required to factor the risk information shared/received via COSMIC into their broader AML/CFT obligations under MAS Notice 626. The requirements pertaining to risk information sharing are set out in Part 4A of the Financial Services and Markets Act 2022 and the MAS Notice FSM-N02 Prevention of Money Laundering and Countering the Financing of Terrorism - Financial Institutions' Information Sharing Platform.

IA function of a participating FI shall assess the effectiveness of its bank's implementation and controls for COSMIC 👍

Scope of Audit	The IA function of the participating FIs shall have a good understanding of the specific changes to existing internal policies, procedures, systems, and controls necessary to comply with the COSMIC requirements. The scope of audit of the AML/CFT procedures, systems, and controls of the participating FIs shall include the usage of COSMIC and the FIs' compliance with the requirements and conditions for information sharing. Examples of areas of focus may include, without limitation, the accuracy and completeness of the risk information disclosed by the participating FIs, timeliness of such disclosures (i.e., whether it was made within the prescribed time periods), whether information request and disclosures by the FIs meet the necessary conditions, the adequacy of the screening process against the platform listing, and the adequacy of controls to safeguard platform access and security of platform information. The scope of audit may also, as needed, include a review of whether pertinent risk information obtained from COSMIC has been duly taken into account in the FI's ML/TF risk assessment considerations of its customers.

5. External Audit

5.1 Focus Areas

This section highlights the four focus areas that could help strengthen AML/CFT outcomes by EA firms. The baseline standards and best practices are set out for each area.

1 *Risk Assessment*

This sub-section addresses the scope and methodology on providing timely risk-based audit review on the AML/CFT control environment, including current in-use data analytics.

2 *Training and Upskilling*

This sub-section addresses the need for specific AML/CFT SMEs within their team, and regular tailored AML/CFT trainings for external auditors involved in AML/CFT audit.

3 *Partnering with Internal Audit Functions*

This sub-section addresses the consideration of IA function's AML/CFT work performed as part of EA firm's risk assessment.

4 *Nature and Extent of Work to be Performed by External Audit Firms during Annual Audit*

This sub-section addresses the areas of consideration when determining the nature and extent of AML/CFT review to be performed.

5.2 Focus Area 1: Risk Assessment

Outcome Statement

EA firms shall perform adequate risk assessment of the bank at planning stage and on an ongoing basis before commencement of audit to determine areas of coverage for AML/CFT work to be performed.

Baseline Standards

- Obtain an understanding from management of bank auditees to ascertain any material changes that may impact the ML/TF risk profile of the bank. Refer to 2.3 Focus Area 1: Risk Assessment for the list of areas for consideration when assessing ML/TF risk profile of the bank. Discuss with management to identify any heightened ML/TF risks or areas of concern since the last audit that shall be considered for inclusion in the current audit scope.

- Enquire if there have been any of the following AML/CFT reviews/inspections conducted on the bank:
  - MAS inspection or supervisory visit or concerns raised by MAS
  - IA (including local, regional or group review performed)
  - Independent reviews commissioned by MAS on the bank
  - Others (e.g., home country regulator inspection review)

  Refer to Appendix A: Examples of Areas for Consideration When Assessing Anti-Money Laundering and Countering the Financing of Terrorism Reviews/Inspections Performed on Bank Auditees during the External Audit Planning Phase, for list of areas for consideration when reviewing AML/CFT reviews/inspections performed on banks.

- Review latest EWRA conducted by the bank as part of the EA firm's risk assessment to identify areas of risks, including those associated with new products/services/client offerings and customer segments. Understand and evaluate the committee(s) within the bank that deliberates on AML/CFT related matters (including overdue CDD reviews, TM alerts etc), and its oversight over issues (including those from QA testing performed) identified from Lines 1, 1.5 and 2 on AML/CFT matters. Assess whether key AML/CFT metrics are included in the Management Information System ("MIS") reporting to senior management (and board, if required)

- Obtain and review the bank's gap analysis against existing AML/CFT regulations, as well as recent circulars and guidance issued by the MAS and ABS. This is to ensure gaps (if any) are timely and completely identified with clear action plans to close the gaps, and timely updated to senior management on the remediation status of the gaps.

- Maintain regular updates with the MAS on both generic and bank-specific areas of concerns and the need for additional coverage, where relevant, taking into consideration MAS' Comprehensive Risk Assessment Framework and Techniques assessment of the bank.

- At commencement of work, EA firms shall consider any changes in circumstances and the need to revisit the risk assessment and scope of work established at planning stage.

5.2 Focus Area 1: Risk Assessment

Best Practices

Review EWRA	• Review the bank's EWRA in detail to establish that the risk assessment is robustly performed, taking into consideration all the relevant risk factors, and is clearly documented and up to date. • Identify and assess the aging and reporting of issues (including those from QA testing performed) raised by Lines 1, 1.5, and 2, and other review functions to key governance forums.
Use of DA	Deploy DA to perform ML/TF risk assessment of the bank auditees. To the extent practical and effective, external auditors may also consider the baseline standards and best practices specified in "2.4 Focus Area 2: Scope and Methodology" of the IA section.

5.3 Focus Area 2: Training and Upskilling

Outcome Statement

EA firms[9] involved in the AML/CFT work shall be adequately equipped with the necessary AML/CFT knowledge and skillsets to conduct an effective and robust AML/CFT audit. General financial audit function in the EA firms shall try to identify specific AML/CFT SMEs within their team.

Baseline Standards

The following shall be considered:

- Conduct annual in-house AML/CFT training for external auditors involved in the audit of banks. The EA firm shall determine the number of hours allocated to AML/CFT trainings to make sure that the team is equipped with the required knowledge.
- Scope of training shall be tailored according to staff experience and skill sets.
- Involve the EA firm's AML/CFT SMEs to facilitate the annual in-house AML/CFT training.
- Consider including the following in the scope of the AML/CFT training:
  - Emerging trends such as cryptocurrencies and VASPs (where relevant) and typologies in ML/TF
  - New/amended MAS and FATF requirements
  - Specific product knowledge/industry players (e.g., cryptocurrencies and VASPs) where relevant
  - Culture and control awareness such as identification of red flags including the follow up actions to be taken
- Training materials/methodology shall include:
  - Case studies and examples for illustration
  - Quiz to ascertain effectiveness of training

Best Practices

Deployment of AML/CFT SMEs	For more complex bank audits, some EA firms deploy their AML/CFT SMEs instead of the general financial audit team. If the latter has to be considered, regular consultations with the specialized AML/CFT SMEs are held to ensure key ML/TF risks are considered.
Professional Certifications[10]	As a value add, some EA firms sponsor their AML/CFT team members for external AML/CFT certifications. Some examples include: • CAMS • Advanced CAMS – Audit Certification • ICA Diploma in Financial Crime Compliance (Singapore) • ICA Advanced Certificate in Regulatory and Financial Crime Compliance (Singapore) • Singapore University of Social Sciences - Certificate course on Financial Crime Compliance • Other relevant IBF-STS accredited programs for AML/CFT

To the extent practical and effective, EA firms may consider the baseline standards and best practices specified in "2.5 Focus Area 3: Training and Upskilling" of the IA section.

[9] EA firms may deploy their AML/CFT SMEs or general financial audit team to perform AML/CFT work. For purposes of "Focus Area 2: Training And Upskilling", the term "external auditors" refers collectively to both AML/CFT SMEs and general financial audit team. As the set-up of each EA firm may vary, it is left to the discretion of each EA firm to determine what constitutes a "SME" as long as these individuals are conversant with AML/CFT regulatory requirements.

[10] Refer to Appendix F for examples of IBF-STS accredited programs.

5.4 Focus Area 3: Partnering with Internal Audit Functions

Outcome Statement

EA firms shall consider the relevant AML/CFT work performed by the IA function for purposes of risk assessment. To the extent possible, EA firms may consider the feasibility of drawing comfort from AML/CFT work performed by the IA function.

Baseline Standards

- Obtain and review AML/CFT reports issued by the IA function during the year.
- Understand the scope of work performed by IA function and its impact on the EA firm's AML/CFT work if an AML/CFT review was conducted in the last year:
  - Identify the business unit(s) covered, including any inherently higher risk segments or products that were in-scope
  - Determine the areas covered and whether coverage included minimally CDD and ongoing monitoring
  - Determine the timeframe covered for the review
  - Review the outcome of review performed
  - Assess the proposed plans by the bank to remediate/resolve issues identified, including timeline for implementation.

  It should be noted that the above should be considered regardless of whether the EA firm plans to draw comfort from the work performed by the IA function.
- Understand from the IA function whether there have been any concerns/issues noted from its AML/CFT review.
- Discuss with Audit Committee whether there are any concerns with leveraging AML/CFT work performed by the IA function.
- Evaluate the reliability and adequacy of the IA function's work to determine whether the EA firm can draw comfort from the work done. See Appendix B: Examples of Areas for Consideration When Assessing Whether External Audit Firms can Consider the Work Performed by Internal Audit Functions for specific areas for consideration.
- Assess if there are material or "hot spot" risk areas that Audit Committee may require additional, independent assurance to ascertain the robustness of controls. In such cases, the EA firm and IA function may agree to cover the same areas in their respective audits. Examples of higher risk customer segments or activities include private banking and trade finance. Some areas for attention include:
  - Areas where Audit Committee may want the EA firm to compare the bank's standards against industry practices
  - Areas focused by regulators
  - Emerging risk areas that regulators may have alerted industry to focus on
- Communicate the decision to IA function and Audit Committee in the event the EA firm chooses to draw comfort from the work performed by the IA function to prevent "circular referencing to each other".

Best Practices

Joint Walkthrough between IA Function and EA firms	In certain cases where both parties cover the same areas, the EA firms perform joint walkthroughs with the IA function to align understanding and reduce the duplicated efforts for bank stakeholders.

5.5 Focus Area 4: Nature and Extent of Work to be Performed by External Audit Firms during Annual Audit

Outcome Statement

EA firms shall ensure adequate coverage for AML/CFT work while adopting a risk-based approach.

Baseline Standards

- EA firms shall substantiate the coverage and basis of sample sizes selection for the AML/CFT work on a risk-based approach, with due consideration of the baseline standards and best practices specified in this paper.

- For banks which have identified areas that pose inherently higher ML/TF risk, regardless of whether reviews/inspections have been performed by the IA function, regulators, or other independent reviewers, EA firms shall consider reviewing minimally, their CDD and ongoing monitoring processes during the annual audit and governance, including escalation and aging of AML/CFT issues (including those from QA testing performed) raised internally across the bank's Lines 1, 1.5 and 2. Refer to Appendix C: Examples of Key Areas to be Covered by External Audit Firms for the key areas that can be considered by EA firms for the review.

  In the event the EA firms choose not to cover the above for banks deemed to pose inherently higher risk, the assessment on why this is not performed shall be documented.

- For banks which have identified areas where ML/TF risk is not highlighted as a significant risk, EA firms shall still consider performing AML/CFT work annually, rotating the areas to be reviewed and tested each year.

  Refer to Appendix C: Examples of Key Areas to be Covered by External Audit Firms for the key areas that can be considered by EA firms for the review.

- EA firms shall adopt a risk-targeted approach when selecting samples for CDD review (rather than on a random basis). Refer to Examples of Higher Risk Customers for examples of higher risk customers for consideration.

- For clarity in scope and extent of coverage in the Audit Long Form Report, EA firms shall clearly set out the AML/CFT coverage for the year and specify the areas/control processes where sample testing has been conducted to determine effectiveness of controls. They shall also indicate where the EA firm had drawn comfort from the audit work performed by third parties. Refer to Example of Documentation of Anti-Money Laundering and Countering the Financing of Terrorism Coverage in Audit Long Form Report for an example of the write-up with respect to AML/CFT coverage by EA firms.

- EA firms shall consider whether any follow-up is necessary for findings raised from MAS inspections performed on the bank. Factors for consideration include the following:

  - Whether MAS has mandated an independent party to be appointed to review the remedial actions taken by the bank (refer to IA Focus Area 4: Reporting and Follow-up on Findings).
  - Whether remedial actions have been completed at the point of commencement of the EA firm's review.
  - Whether the IA function is performing a follow-up review (refer to EA Focus Area 3: Partnering with Internal Audit Functions).

5.5 Focus Area 4: Nature and Extent of Work to be Performed by External Audit Firms during Annual Audit

Best Practices

Governance	Some EA firms assessed the timeliness of issues identified by the bank's own QA assurance testing being escalated to mid-level forums/committees, and noted areas where banks could have acted on earlier and/or where internal identified issues could have escalated to more senior forums/committees for additional scrutiny and actions to be undertaken.
Use of Tools	Some EA firms have deployed the use of tools in its AML/CFT work (such as for DA purposes). However, the feasibility of this approach is dependent on availability of data provided by the bank and information technology security protocols on deployment of tools onto the bank's IT infrastructure (assuming the data used for analysis resides on the bank auditee's environment).
Use of DA	EA firms have traditionally faced challenges in deploying the use of DA for AML/CFT work due to sensitivity of sharing of information with external auditors outside of the bank's IT infrastructure (i.e. sending such client information to the external auditor directly) and/or technology challenge in deploying DA tools onto the bank's IT infrastructure for DA work. Notwithstanding the above, EA firms are encouraged to consider the adoption of DA for purposes of AML/CFT work. To the extent practical and effective, external auditors may also consider the baseline standards and best practices specified in "2.4 Focus Area 2: Scope and Methodology" of the IA section.
Approach for Audit of Central/ Overseas AML Functions	For banks with central/outsourced overseas AML/CFT functions, some EA firms have included the following considerations when assessing the use of overseas teams/offices: • Determine whether the review and testing should be performed by the EA firm in Singapore if the area is deemed to be a higher risk area • Assess whether testing should be conducted by the EA firm in Singapore if there are no appropriate or competent overseas counterparts who can perform the review and testing on behalf of the EA firm in Singapore. • Evaluate the competency of the overseas EA team/office, particularly their familiarity with Singapore requirements, if review and testing is performed by an overseas team/office. • Consider issuing documented instructions to ensure clarity in the scope to be covered if the review and testing needs to be carried out by an overseas EA team/office.
Unpredictability testing	Some EA firms incorporated "unpredictability" testing in the AML/CFT area (e.g. selecting low risk customers for review instead of focusing only on high-risk customers) for comprehensiveness.

6. Conclusion

Banks' IA functions and EA firms play key roles in ensuring that banks' internal policies, procedures, and controls remain effective to combat ML/TF risks and are in compliance with regulatory requirements. It is important for the banks' IA functions and EA firms to be equipped to provide sufficient assurance that the banks' ML/TF risk controls are able to keep pace with the evolving ML/TF risk landscape, and possible shifts in business strategy and environment.

This paper is intended to help internal and external auditors by setting out baseline standards and best practices for them to consider when determining the appropriate scope and extent of testing in the conduct of AML/CFT audits for banks. Internal and external auditors are also encouraged to consider the use of DA and new techniques to strengthen their AML/CFT audit effectiveness. AAPG noted that DAs are already being used by some banks with good outcomes and has set out some specific case studies in this paper as a reference.

Banks' IA function and EA firms shall review their existing audit practices against this paper and consider if there are areas that they can enhance to raise their AML/CFT audit effectiveness. Internal and external auditors are encouraged to continue to share best practices with industry bodies and peers to uplift AML/CFT standards within the industry. Collectively, the audit industry can further strengthen banks' resilience against ML/TF risks.

Appendix A: Examples of Areas for Consideration When Assessing Anti-Money Laundering and Countering the Financing of Terrorism Reviews/Inspections Performed on Bank Auditees during the External Audit Planning Phase

SN	Categories	Areas for consideration
1	**Timeframe**	• When was the review performed • Have issues raised been remediated/resolved • If issues have been remediated/resolved, has sufficient time elapsed since implementation for EA firms to perform review and testing
2	**Actions Taken by the Bank**	• Was there an independent party appointed by the bank to remediate issues raised • Did the bank appoint an independent party to perform review of the remediation actions taken by the bank to remediate/resolve issues raised

Appendix B: Examples of Areas for Consideration When Assessing Whether External Audit Firms can Consider the Work Performed by Internal Audit Functions

SN	Categories	Areas for consideration
1	**Adequacy of Scope Covered**	• Did the scope cover any material changes in business, customer segments, and products and services offering during the period of review • For areas deemed higher risk, have the IA function also covered these areas • Did the IA cover AML/CFT functions outsourced to other locations • If the IA is performed by an overseas team, is it explicit that the Singapore entity is covered
2	**Independence of IA Function**	• Is the IA function independent from management (refer to reporting lines)

3	**Competency of IA Function in the Area**	• Is the IA function adequately resourced with AML/CFT SMEs
		• Was the IA review covered by team members who are in Singapore and familiar with MAS requirements
		• Are there any concerns with the competency and quality of the IA function from prior experience, such as:
		  • Whether the IA function comprises appropriate AML/CFT SMEs or is it made up of only general internal auditors
		  • Adequacy of team composition
		  • Whether the findings raised previously by the IA function correspond to that raised by the EA firm, regulators etc.
		  • Whether the IA function is residing in Singapore and are well versed in Singapore requirements

4	**Timing of IA Function's Work**	• Is the audit already completed at the point of commencement of EA firm's planning • Does the period of coverage by the IA function overlap with the financial year audit by the EA firm • If the work of the IA function has yet to commence at the point of commencement of EA firm's planning, it is unlikely that the EA firm can rely on the IA function's work performed
5	**Discussion with MAS**	• Any concerns raised by MAS on the IA function's work

Appendix C: Examples of Key Areas to be Covered by External Audit Firms

SN	Categories	Areas for consideration
1	**EWRA**	• Whether there is an EWRA framework established • Whether the EWRA is performed on a timely basis • Whether the EWRA includes all businesses, products and services offerings, customers segments served by the bank etc.

2	**CDD**	• Whether the bank has put in place appropriate framework, policies, and procedures on how CDD should be performed, including identification and verification, name screenings, and risk assessment
		• Timeliness of CDD performed, both at onboarding and ongoing basis
		• For samples reviewed (including for periodic review and trigger event review), to consider looking at the following:
		  • Whether identification and verification have been performed on key parties to an account (may refer to beneficial owners, authorised signatories, connected parties etc.)
		  • Whether name screening had been performed on required persons/names
		  • Whether ML/TF risk rating is appropriate
		  • Whether account has been approved by the right person
		  • Timeliness of review performed
		  • Whether SOW and SOF corroboration practices are robust and adequately performed (e.g., whether adequate and good quality corroborative evidence was obtained; whether the SOW assumptions used in benchmarking were prudent, and whether there was a reasonable degree of reliance placed on customer representations, etc.)
		  • Tax risk indicator and whether this has been taken into consideration for ML/TF risk assessment

3	**Name Screening**	• Whether the bank has put in place guidance on which are the parties to an account that needs to be screened, when screenings need to be performed, expected documentation for name screening hit disposal, escalation protocols for name screening hits, approach for name screening hits that cannot be resolved etc. • Whether the name screening hits are reviewed and disposed on a timely basis • For banks that adopt a name screening system, whether there are regular reviews performed on the effectiveness of system parameters adopted • Completeness of information sources used for name screening

Appendix C: Examples of Key Areas to be Covered by External Audit Firms

SN	Categories	Areas for consideration
4	**Wire Transfers**	• Whether the bank has put in place appropriate framework, policies, and procedures on what needs to be screened for wire transfers, when screenings need to be performed, when it needs to enquire for further information and rationale for transactions, escalation protocols etc • Whether screening hits are reviewed and disposed on a timely basis

5	**Suspicious Transaction Reporting**	• Whether the bank has put in place appropriate framework, policies, and procedures on post-mortem actions to be undertaken post STR filing
		• Timeliness of STR filings
		• For samples reviewed, to consider looking at the following:
		  • Accuracy and completeness of information populated in the Suspicious Transaction Reporting Office Online Notices And Reporting ("SONAR") platform against investigation performed by the bank
		  • Timeliness of STR filed
		  • Post-mortem actions taken duly address the risks identified

6	**TM**	• Whether the bank has put in place TM framework, policies, and procedures with respect to timeframe for investigation/clearance of alerts, how alerts should be escalated as necessary
		• Whether the bank has in recent year(s) performed a review of its TM scenario, parameters and thresholds for effectiveness
		• Whether clearance of TM alerts are performed on a timely basis
		• For samples reviewed, to consider looking at the following:
		  • Whether the alerts are cleared on a timely basis
		  • Whether the alerts are properly dismissed and documented
		  • Whether appropriate post-mortem actions have been performed

7	**Governance and Oversight**	• Whether there is a committee within the bank that deliberates AML/CFT related matters (including overdue CDD reviews, TM alerts etc.) • Whether key AML/CFT metrics are included in the MIS reporting to senior management (and board, if required)
8	**Trainings**	• Whether there are regular AML/CFT refresher trainings for its staff • Whether there are timely AML/CFT trainings for its new joiners • Whether AML/CFT trainings are tailored to the roles undertaken by each department (i.e., are they fit for purpose)

Appendix D: Examples of Higher Risk Customers

SN	Categories	Areas for consideration
1	**Customers**	• Family offices • Complex structures which may not be reasonably explained • Foreign PEPs
2	**Products, Services, and Transactions**	• Correspondent banking services • Trade finance products • Private banking • Remittances • Money changer
3	**Channels**	• Non-face-to-face, including digital channels of onboarding • Accounts managed outside of Singapore and booked into Singapore
4	**Geographies**	• Customers, trade and products based in higher risk countries (e.g., FATF rating, Global Organised Crime Index, Global Terrorism Index etc.)

The EA firm can also refer to the “National Risk Assessment” issued for references of higher risk areas.

Appendix E: Example of Documentation of Anti-Money Laundering and Countering the Financing of Terrorism Coverage in Audit Long Form Report

EA firms should set out their approach and scope for their AML/CFT audit of the bank that includes the following:

- Understanding the relevant AML/CFT policies and procedures adopted by the bank
- Establishing an approach to ensure adequate sampling for higher risk areas within the audit scope, including the rationale for having more samples in specific business segments.
- Obtaining and reviewing samples of CDD performed for newly on-boarded customer accounts against the bank's policies and procedures
- Reviewing the current framework in relation to TM scenarios, thresholds and parameters
- Obtaining and reviewing samples of TM alerts to understand the timeframe, documentation of assessment and rationale for closure of alerts
- Obtaining and reviewing samples of transactions (e.g. trade finance) against the bank's policies and procedures, where applicable
- Obtaining and reviewing samples of STRs not filed during the financial year and understanding the post-mortem actions taken for these accounts if applicable
- Understanding the gap analysis performed by the bank against new/amended AML/CFT requirements as well as guidance and circulars issued by the MAS since the last audit
- Including additional scope of work beyond the baseline areas mentioned above, along with the considerations behind their inclusion (e.g., arising from a request from the bank's Audit Committee, the EA firm's risk assessment of the bank during the planning stage, or the validation of MAS inspection findings).

Appendix F: Examples of The Institute of Banking and Finance Standards Training Scheme Accredited Programs

IBF Approved Financial Training Provider	IBF-STS Accredited Programs
ACAMS	Certified Anti-Money Laundering Specialist (CAMS) – 6th Edition – Singapore (CAMS6-SG)
International Compliance Training Academy Pte Ltd	• ICA Advanced Certificate in Regulatory and Financial Crime Compliance • ICA Diploma in Governance, Risk and Compliance • ICA Diploma in Anti-Money Laundering/Counter Financing Terrorism (AML/CFT) • ICA Diploma in Financial Crime Compliance
Singapore University of Social Sciences	FIN573 Financial Crime Compliance
Wealth Management Institute Limited	Advanced Diploma in Financial Crime Compliance and Compliance Analytics

Appendix G – Glossary

Acronym	Description
AAPG	Anti-Money Laundering Audit Peer Group
ACIP	AML/CFT Industry Partnership
AEs	Audit Entities
AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
CAATs	Computer-Assisted Audit Techniques
CAMS	Certified Anti Money Laundering Specialist
CDD	Customer Due Diligence
CDTs	Case Disposition Templates
COSMIC	Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases
CRF	Customer Risk Framework
DA	Data Analytics
EA	External Audit
EBRs	External Business Relationships
EWRA	Enterprise-Wide Risk Assessment
FATF	Financial Action Task Force
FIs	Financial Institutions
IA	Internal Audit
IBF-STS	Institute of Banking and Finance Singapore's Standards Training Scheme
ICA	International Compliance Association
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MIS	Management Information System
ML/TF	Money Laundering and Terrorism Financing
MSB	Money Service Business
NLA	Network Link Analysis
NLP	Network Link Processing
PEP	Politically Exposed Person
PF	Proliferation Financing
PUP	Product Usage Profiles
QA	Quality Assurance
SMEs	Subject Matter Experts
SOF	Source of Funds
SONAR	Suspicious Transaction Reporting Office Online Notices And Reporting
SOW	Source of Wealth
STRs	Suspicious Transaction Reports
TM	Transaction Monitoring
VASP	Virtual Assets Service Provider

Annex A – Working Group Members and Other Contributors

Bank	Representative
DBS	Derrick Goh (Co-Chair)
OCBC	Harry Lim (Co-Chair)
Citi	Marcus Ng
Citi	Cherry Chai
Citi	Tan Yan Ling
DBS	Gladys Lee
DBS	Leslie Gan
DBS	Lum Soo Fung
DBS	Elaine Chong
DBS	Ng Wei Khim
DBS	Sia Puay Khim
DBS	Mohamed Siddiq Mohamed Taib
DBS	Tan Tai Hiem
GS	Monica Lim
GXS	Connie Goh
GXS	Teo Kah Fook
GXS	Hannah Liu
HSBC	Ahmer Ramzan
HSBC	Manikandan Shunmugasundaram
HSBC	Paryant Kirtikumar Buch
MariBank	Henry Chan
MariBank	Claire Ong
MariBank	Brian Wong
OCBC	Chow Lai Lin
OCBC	Edwina Goh
OCBC	Tan Wein Dhee
OCBC	Agnes Loh
OCBC	Png Hui Yu
SCB	Tan Eng Ngee
SCB	David O'Brien
UBS	Viral Sanghani
UBS	Marcel Altermatt
UBS	Charlene Su
UOB	Vincent Cheong
UOB	Adrian Chiang
UOB	Cherie Ong

Annex A – Working Group Members and Other Contributors

Observers	
Monetary Authority of Singapore	Ian Lee
Monetary Authority of Singapore	Rachel Huen
Monetary Authority of Singapore	Eunice Ng

Industry Associations	
Institute of Internal Auditors Singapore	Richard Chris Dyason
The Institute of Singapore Chartered Accountants	Fann Kor
The Institute of Singapore Chartered Accountants	Alice Tan

Professional Services	Representative
Internal Audit	
EY	Radish Singh
EY	Nicholas Sebastian
EY	Anamika Guha Thakurta
EY	Janell Joseph
EY	Eunice Aw
PwC	Yura Mahindroo
PwC	Germaine Huang
External Audit	
PwC	Yura Mahindroo
PwC	Germaine Huang
BDO	Tei Tong Huat
Deloitte	Serena Yong
EY	Radish Singh
EY	Christine Lee
EY	Lucretia Aik
KPMG	Chen Junwei
KPMG	Jessie Tay
Mazars	Mark Chew