ACAMS® | Advancing Financial Crime Professionals Worldwide

The ML/TF Risk Assessment—Is it fit for purpose?

Aub Chapman, CAMS

1. Executive Summary

Deficiencies in money laundering/terrorist financing (ML/TF) risk assessments continue to feature as a major issue in enforcement actions by anti-money laundering/counter-terrorist financing (AML/CTF) regulatory authorities in many countries. This is despite the apparent level of maturity of the AML/CTF regime in many individual countries. These deficiencies are a major concern as the primary purpose of an ML/TF risk assessment is to be instructive in the development of an AML/CTF risk management framework. This framework should be relevant and proportionate to the ML/TF risk that a reporting entity may reasonable expect to face through its business activities. The regulatory expectation is that each reporting entity will have applied the appropriate resources and expertise in developing its ML/TF risk assessment, which categorizes its customer types, products and services, delivery channels and jurisdictions as presenting a high, medium or low potential risk for ML/TF.

This paper seeks to provide AML/CTF compliance officers and AML/CTF auditors with some key issues that should be considered when assessing whether or not the ML/TF risk assessment is "fit for purpose."

In doing so, this paper seeks to answer the following questions:

- What skills/expertise/experience and resources are used in developing an understanding of the elements/factors that should be considered in an ML/TF risk assessment which is appropriate and relevant to the business?
- How should an auditor satisfy himself/herself that the reporting entity has applied the appropriate level of resources and expertise in developing, implementing and maintaining its ML/TF risk assessment?

These questions are premised on the following assumptions which are based on the author's own experience in undertaking numerous AML/CTF audits over a wide range of entities that have AML/CTF obligations.

- ➢ The development, implementation and maintenance of an ML/TF risk assessment that is relevant and appropriate to the business activities of the organization is critical to the manner in which the organization manages its ML/TF risks.
- ➢ An ML/TF risk assessment that is deficient in coverage or inappropriate will not provide a sound basis upon which a robust and relevant AML/CTF risk management framework—including its AML/CTF program, operational procedures, processes and systems controls can be developed, implemented and maintained.

2. The Issues and Challenges

2.1 Diversity of industry sectors that have obligations under AML/CTF legislation

On a global level, the importance of the ML/TF risk assessment to developing, mitigating and managing ML/TF risks is clearly demonstrated by FATF Recommendation Number 1, "Assessing risks and applying a risk-based approach" at the national level. The interpretive note to Recommendation Number 1 states in part:

> "In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering risks."[1]

The legal framework, cultural norms and the maturity of financial and IT systems have a major influence on the manner in which individual countries apply a risk-based AML/CTF regime. The diversity of the entities that have obligations also present challenges in developing an AML/CTF risk-based control framework that is relevant and proportionate to the ML/TF risk that the various reporting entities may face. The definitions in the glossary to the FATF Recommendations illustrate the wide range and diversity of businesses that are (or should be) subject to a country's AML/CTF regime. The definitions for "financial institution" and "designated non-financial businesses and professions" contain lists of various business types and functions. While large multinational financial institutions undertake a considerable number of the activities listed, at the other end of the spectrum there are numerous small businesses that undertake a limited number of those activities. To further illustrate this diversity, the home page of the FinCEN website contains a series of drop-down boxes covering:

- Depository institutions
- Casinos
- Money services businesses
- Insurance
- Securities/futures
- Precious metals/jewellery
- Mortgage company/broker

Within each of these categories, there are large, medium and small businesses. It is difficult to quantify the proportion that each represents in the total population of reporting entities within an individual country. However, the Australian environment does illustrate that there are far more small businesses impacted by AML/CTF legislation than larger/well-resourced

[1] Interpretive Note No 2 to Recommendation No 1. The FATF Recommendations – February 2012

businesses. At the end of the 2014/15 year, there were 14,040 reporting entities enrolled with AUSTRAC.[2] Of this total, 5,379 were included in the Remittance Sector Register (i.e., MSBs).[3] Of the 14,040 reporting entities, only 168 were approved deposit-taking institutions.[4] These figures suggest that a substantial proportion of the enrolled reporting entities are small to medium-sized organizations and in relation to the remittance sector, the vast majority of the 5,379 fall into the very small "mom-and-pop" type businesses.

Informal research suggests that in other jurisdictions, the small business sector—which usually provides a very limited number of products/services to customers—also represents a substantial proportion of the reporting entity population.

2.2 Resources and expertise

During and subsequent to the global financial crisis (GFC), regulatory authorities (such as the OCC) have expressed concerns that financial institutions have not employed sufficient and suitably qualified/experienced staff to a level that is appropriate to manage the ML/TF risk that those financial institutions face. The seniority of the compliance staff has also been of concern to the authorities.

In a number of recent enforcement actions resulting in civil money penalties, the failings documented in the published assessment includes commentary on inadequate resources and lack of knowledge and expertise. The following quotes illustrate this ongoing concern:

- "Failed to adequately staff the BSA compliance function at the Bank with personnel to ensure day-to-day compliance with the BSA. The unit responsible for monitoring the Bank's domestic and foreign retail customer accounts was understaffed, and personnel lacked the requisite knowledge and expertise to adequately perform their duties."[5]
- "The Bank's BSA officer and Compliance officer were unqualified for their positions. The BSA and compliance officers held other full-time positions within the Bank, did not have experience with or training in BSA requirements, and spent minimal time dealing with BSA matters."[6]
- "Failed to adequately staff the BSA compliance function at the Bank, with individuals responsible for coordinating and monitoring day-to-day compliance with the BSA. The AML Investigative Services unit responsible for monitoring the Bank's correspondent relationships with foreign financial institutions was understaffed,

[2] The Australian Transaction Reports and Analysis Centre (AUSTRAC)
[3] AUSTRAC Annual Report 2014-15
[4] Australian Prudential and Regulatory Authority website – last viewed 14 Jan 2016
[5] FinCEN assessment of civil money penalty - Number 2011-7
[6] FinCEN assessment of civil money penalty – Number 2010-3

> and personnel lacked the requisite knowledge and expertise to adequately perform their duties."[7]

These three examples involve banks which have had Bank Secrecy Act (BSA) obligations for a number of years. Yet they still failed to meet key AML/CTF obligations and would have been (or should have been) subject to AML/CTF audits over a number of years. If these adverse findings are still being found within what can be described as a mature banking sector, it is not unreasonable to suggest that similar deficiencies exist across the entire reporting entity population. The issue of a non-dedicated compliance staff becomes an even bigger issue for smaller businesses with limited resources and financial capacity and where the obligation for compliance with AML/CTF legislation is not understood or appreciated.

3 Author's Research

To aid the value and insight of this paper, the author recently undertook an informal survey involving telephone and face-to-face interviews with 24 AML/CTF consultants and AML/CTF auditors. This group included independent consultants/auditors and practice leaders or experienced members of AML/CTF teams within major firms such as EY, KPMG, PwC and Deloitte. The objective was to gather a range of opinions on how consultants and auditors viewed reporting entities' management of their AML/CTF obligations.

As expected from any small sample survey, the findings represented the individual interviewees' experience in undertaking AML/CTF audits. The interviewees indicated that their AML/CTF audit assignments covered a wide cross-section of reporting entities ranging from large financial institutions operating across multiple jurisdictions through to small locally operating businesses.

For the purposes of this paper, large financial institutions are defined as major financial institutions that operate across multiple jurisdictions and major financial institutions that operate within one jurisdiction. The business activities of these financial institutions are structured across various business streams which focus on specific market segments (e.g., institutional banking, corporate banking, business banking, mass-market/retail banking, wealth management, etc.). In almost all cases each of the operating divisions within these financial institutions offer a wide range of products and services that are captured under AML/CTF legislation. While a growing number of these major financial institutions have adopted (or are adopting) an enterprise-wide approach to the ML/TF risk assessment, a number appear to have created division-specific ML/TF risk assessments. Dedicated AML/CTF resources are deployed across these institutions. Although the number and experience of the AML/CTF resources is often questionable relative to the ML/TF risks that the entity may reasonably face.

[7] FinCEN assessment of civil money penalty – Number 2010-1

However, many businesses that only offer one or two services are also caught under AML/CTF legislation. In most cases, functions caught under AML/CTF legislation represent only a small portion of the business's activities. The survey interviewees indicated that many small businesses are managing their AML/CTF obligations on a part-time, non-dedicated resource basis. As such, these resources have limited AML/CTF expertise and experience. A key concern is that many have little, if any, understanding of the ML/TF risks their business may reasonably expect to face. This manifests itself into poorly structured and deficient ML/TF risk assessments.

An additional concern is that in many cases external AML/CTF expertise has been engaged to develop and implement an appropriate ML/TF risk assessment and AML/CTF risk management framework for the reporting entity. It appears that these AML/CTF policies/programs and associated procedures, processes and system controls have been accepted at face value with little or no ownership or understanding of the implications by the reporting entities' management and staff.

4 Utilizing Publicly Available Resources

4.1 The use of typologies, case studies and enforcement actions in developing/enhancing and maintaining the ML/TF Risk assessment

At the global level, an ever-increasing body of high-quality ML/TF typologies, sanitized case studies and ML/TF risk trends reports are published as an aid to affected industry sectors in understanding their relevant ML/TF risks. The published materials are an essential source in the development of an ML/TF risk assessment that is appropriate to an individual reporting entity's ML/TF vulnerabilities.

The FATF website contains an extensive library of sector-specific ML/TF risk reports and ML/TF typologies reports. These are produced on a regular basis and updated when new ML/TF risks emerge. While it is now some years since FATF produced an excellent report on risk management strategies,[8] that document remains extremely relevant in the context of both national and individual entity ML/TF risk assessments. As an example of sector-specific reports, FATF has published a report covering money remittance and currency exchange providers.[9] Another example is the FATF report covering new payment methods.[10]

These reports are comprehensive and well structured. To a person responsible for AML/CTF compliance within an organization, the time needed to comprehend these in combination with the officer's other duties is a real challenge. It is not always easy to adequately accommodate both within the available time.

---

[8] FATF Report – Money Laundering & Terrorist Financing Risk Assessment Strategies – June 2008
[9] FATF Report – Money Laundering through Money Remittance and Currency Exchange providers – June 2010
[10] FATF Money Laundering Using New payment Methods – October 2010

In addition to the body of helpful information/guidance produced by FATF, FATF-styled regional bodies have also committed considerable time and resources in developing and publishing a wide range of reports, many of which are sector-specific. The regional bodies also conduct annual typologies workshops which tend to focus on specific existing or emerging ML/TF risks. Often these reports provide information which financial institutions will find to be of value beyond AML/CTF. In conjunction with the Council of Europe's Global Project on Cybercrime, in 2012, MONEVAL developed and published a typologies research paper titled "Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction." This paper contains some very helpful guidance for reporting entities when considering the distribution channels element of an ML/TF risk assessment and for developing fraud control strategies.

Other international bodies and authorities such as the World Bank Group, the International Monetary Fund, the United Nations Office on Drugs and Crime and the Bank of International Settlement (Basel Committee on Banking Supervision) have all published a number of reports. These provide reporting entities with valuable guidance and information on factors that should be considered when developing an ML/TF risk assessment

Within the private sector, many legal bodies/firms, accounting firms and compliance systems vendors have published numerous AML/CTF-related reports which are accessible on the relevant firms' websites. A number of these documents relate to ML/TF risk assessment methodologies and/or risk assessment tools which have been developed to assist clients. At the industry level, the Wolfsberg Group (which comprises 13 of the world's largest private banks) has produced and published a number of standards which its members are required to comply with. One of these is the "Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption." This document provides valuable guidance for all reporting entities on risk assessment methodologies and key issues that should be considered when developing an ML/TF risk assessment.

Clearly, there is an ever-increasing mountain of information that is available from a variety of sources, including the internet, which can assist compliance officers in developing an ML/TF risk assessment. However, there is a critical need to utilize the information in the context of the entity's business model and business activities. Without a clear understanding of the features of the products and services being offered to customers, the information contained within the types of publicly available documents mentioned above may lead to inappropriate outcomes.

That said, several fundamental problems remain for those developing an ML/TF risk assessment. "Information overload" and the "time required" to identify and search through the relevant publicly available information sources present challenges. This is a large enough challenge for large financial institutions that operate across multiple jurisdictions. It presents a different and even larger challenge for smaller reporting entities with limited and non-dedicated compliance staff. Fortunately, these issues are being addressed by bodies such as ACAMS and the major consulting firms that have developed automated risk assessment methodologies and toolsets that can substantially reduce the need for individual reporting entities (especially smaller reporting entities) to unnecessarily expend valuable resources in developing stand-alone ML/TF risk assessments.

Naturally, there is no "one right answer" to developing, implementing and maintaining an ML/TF risk assessment that is appropriate and proportionate to the ML/TF risks that an individual reporting entity may face. Many larger financial institutions prefer to invest resources in either developing their own ML/TF risk assessment or in engaging the services of an external provider that offers a sophisticated/commercially robust ML/TF risk assessment model.

The cost associated with engaging external expertise is often beyond the financial capacity of smaller reporting entities. In recognition of this problem, a number of AML/CTF regulators/supervisors have published material which is aimed at assisting reporting entities. This material often describes the factors that should be considered when developing and implementing an appropriate AML/CTF risk management framework. Exhibit A is an easy-to-understand schematic published by AUSTRAC that summarizes the elements that should be considered when developing a robust risk management policy and strategy. However, populating the inherent and residual ML/TF risk assessment remains a challenge, especially where there is a lack of skilled AML/CTF resources readily available within the organization.

4.2 The Use of Guidance Notes/Guidelines Issued by Regulators/Supervisors and FIUs

In addition to the plethora of information mentioned in the previous section, many national FIUs and AML/CTF supervisors/regulators continue to produce guidance notes to assist reporting entities in understanding and meeting the relevant authority's expectations. Such guidance often focuses on compliance with obligations under the local AML/CTF regime.

This type of guidance can be industry-wide and general in nature or it can be targeted to an industry subsection (e.g., providers of crowd-sourced equity funding).

While such guidance may not be legally binding, it is wise for reporting entities to take heed of what the supervisor/regulator has published. This can avoid unnecessary friction and debate when the supervisor/regulator undertakes an official compliance assessment.

The author has undertaken AML/CTF audits for a wide variety of reporting entities in several jurisdictions over the past decade. It is interesting to note that, as part of undertaking formal compliance assessments, the compliance testing undertaken by a number of local regulators includes seeking evidence that the reporting entity has had appropriate regard for the guidance and any feedback provided by the FIU and/or regulator. This includes evidence that the board/senior management have been made aware of such guidance/feedback. From an ML/TF risk assessment perspective, it is appropriate to assess both the regulatory risk and the business risk associated with the local AML/CTF regime.

5. The Disconnect between the ML/TF Risk Assessment and the AML/CTF Control Framework

As previously mentioned, the primary purpose of an ML/TF risk assessment is to instruct the development of an AML/CTF control framework that is appropriate and proportionate to the ML/TF risk that a reporting entity may reasonably face. This implies that the ML/TF risk assessment should identify and include all known risks from the customer, product and service, distribution channel and jurisdiction perspectives. The resulting risk ratings should influence the manner in which and the degree to which each risk should be mitigated and managed.

Unfortunately, many reporting entities fail to make the connection between the ML/TF risk assessment and the AML/CTF control framework that is implemented. The following examples illustrate how such disconnections occur, either deliberately or through ignorance and misunderstanding:

- **Risk ratings for different customer types**

  Certain customer types such as trusts, PEPs, complex corporate structures, etc., will be assigned a higher ML/TF risk rating in the ML/TF risk assessment model than (say) retail/mass-market customers. This should trigger a requirement for a higher level of KYC/CDD for those customer types with a higher ML/TF risk rating.

  It is not uncommon, especially in smaller reporting entities, for standard KYC/CDD processes to be applied at onboarding irrespective of the differences identified in the ML/TF risk assessment model.

- **Risk ratings for different product types**

  The ML/TF risk assessment may identify some products as presenting a higher ML/TF risk than others. However, when developing and implementing an enterprise-wide transaction monitoring program, all transactions are subject to the same level of monitoring.

- **Risk ratings for different staff categories**

  In developing the ML/TF risk assessment, certain categories of staff may be identified as presenting a higher level of ML/TF risk than other categories. For example, customer facing staff (e.g., tellers and business development managers) present a high ML/TF risk vulnerability than say IT and compliance staff. However, many smaller reporting entities elect to undertake the same level of employee due diligence due to the low level of staff turnover and to ensure consistency.

6. Challenges for the AML/CTF Auditor

The AML/CTF legislation in many jurisdictions provides for the AML/CTF audit to be carried out by either internal or external staff subject to the audit staff having had no involvement in the development, implementation or ongoing maintenance of AML/CTF risk management framework (including the ML/TF risk assessment). For large financial institutions, this enables the audit function to be conducted by (say) an internal audit department. It is important that the audit department demonstrates independence and competency and often the latter is not present in the resources of the internal audit department.

When an external auditor is engaged to undertake the AML/CTF audit, it is essential for the management of the reporting entity to seek evidence of the competency of the auditor who undertakes the AML/CTF audit. Most legal firms have the requisite knowledge and skills to assess technical compliance with the obligations set out in the relevant AML/CTF legislation. However, for many legal firms, it might often be questionable whether or not the auditor has an appropriate level of understanding of the auditee's business activities to adequately assess that the AML/CTF policies, procedures, processes and system controls are appropriate for the level of ML/TF risk that the business may face. More importantly, a lack of knowledge of the product features and distribution channel components of the client's business may result in a less than acceptable audit assessment.

This brings into sharp focus the challenge facing an AML/CTF auditor who offers audit services across the spectrum of reporting entities that now exist under most countries' AML/CTF regime. Understanding the technical requirements for compliance with the more common AML/CTF obligations (such as employee due diligence) is one thing. Understanding the ML/TF risks associated with features of new and emerging payment system and more sophisticated products that are provided to select groups of customers is another issue. Products and services tailored to suit the needs of individual high-net worth customers often introduce ML/TF risks that have not been identified and reflected in the ML/TF risk assessment.

The need to ensure that all relevant elements have been factored into the ML/TF risk assessment is fast becoming a major component of an effective AML/CTF audit. It is a prerequisite to assessing the appropriateness of the AML/CTF policies, procedures, processes and system controls that make up the overall AML/CTF risk management framework.

Keeping abreast of money laundering and terrorist trends, especially those associated with new and emerging markets is a challenge. Understanding the ML/TF risks associated with digital currencies, crowd-sourced funding, the impact of the globalization of financing markets and the ever-increasing introduction of technologies that provide for faster and cheaper transfers of value has become a necessary core competency of an AML/CTF auditor.

6.1 Some ML/TF Risk Assessment Checklist Thought-Starters for AML/CTF Compliance Officers

Creating and completing a check-list when creating (or reviewing) an ML/TF risk assessment will provide evidence that the right level of skills and experience have been deployed. The following sample set of "thought-starters" may assist the AML/CTF compliance officer in demonstrating that the appropriate level of resources, experience and expertise have been employed:

- Who is (or should be) involved (e.g., compliance, business, risk management, external expertise)?
- Who owns/is responsible for the ML/TF risk assessment?
- Who signs-off/approves the ML/TF risk assessment?
- What publicly available information/resources have been used in understanding ML/TF risks?
- Are all the organization's customer types, product features and distribution channels included?
- Do recent enforcement actions signal key issues that should be considered?
- Does the ML/TF risk assessment methodology align with the enterprise-wide risk management framework/strategy
- Is there "buy-in" from the executive/senior management team?
- Is industry comparison/validation possible?
- How will the currency of the ML/TF risk assessment be maintained?

6.2 Some ML/TF Risk Assessment Checklist Thought-starters for AML/CTF Auditors

The AML/CTF auditor faces similar challenges in understanding the ML/TF risk that a client's business model and activities present.

The AML/CTF auditor must consider what evidence is required and what testing will be undertaken to enable him/her to have a level of confidence that the ML/TF risk assessment is a sound base upon which the client has built its AML/CTF risk management framework.

The following sample set of "thought-starters" may assist the AML/CTF auditor in assessing whether or not the appropriate level of resources, experience and expertise have been employed and that the ML/TF risk assessment is "fit for purpose:"

- Do I have sufficient understanding of the client's business model?

- Do I have information that describes the markets in which the client operates?
- Do I have information that describes the client's customer types, products and services, distribution channels and jurisdictions in which it operates?
- Is there evidence of the publicly available information/documents that the client used in developing its ML/TF risk assessment?
- What additional research should I undertake to ensure all relevant known ML/TF risks have been considered by the client?
- What ML/TF issues have been identified in previous AML/CTF audits and/or compliance assessment by the AML/CTF supervisor/regulator?
- What evidence exists to demonstrate sound governance by the board and executive/senior management?
- What evidence exists to show that appropriate resources were engaged in the development and maintenance of the ML/TF risk assessment?

7. Conclusion

The opinions of the AML/CTF consultants and AML/CTF auditors interviewed and the author's own experience highlight an ongoing concern that many ML/TF risk assessments are not "fit for purpose." Deficiencies in identifying ML/TF risks that are relevant to the business and/or the disconnection between the ML/TF risk assessment (that it is meant to provide direction) and the risk management framework, continue to be widespread. It is only when these issues are addressed that an ML/TF risk assessment can be seen as "fit for purpose."

As with the evolution of the effectiveness assessment component of the FATF Mutual Evaluation Methodology, it will take time to develop a set of suitable measures that are acceptable to management, industry and the authorities to demonstrate that the ML/TF risk assessment is "fit for purpose."

The key objective must be the development of a high quality ML/TF risk assessment that is appropriate and proportionate to the ML/TF risks that a reporting entity may reasonably expect to face. This demands resources that have the necessary level of experience and expertise. It is essential that the supporting information for this is available upon or during an audit of the actual AML/CTF program.

ML/TF risk assessments must be supported by evidence that the appropriate level of resources, experience and expertise have been employed in the development, implementation and maintenance of the ML/TF risk assessment and the resulting AML/CTF risk management framework.

Glossary

ACAMS	Association of Certified Anti-Money Laundering Specialists – *www.acams.org*
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
APG	Asia Pacific Group on Money Laundering – *www.apgml.org*
AUSTRAC	Australian Transaction Reports and Analysis Centre which is Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulator and specialist financial intelligence unit (FIU) – *www.austrac.gov.au*
BSA	Bank Secrecy Act
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force – *www.fatf.gafi.org*
FinCEN	Financial Crimes Enforcement Network – *www.fincen.gov*
GFC	Global financial crisis
ML/TF	Money Laundering / Terrorism Financing
MLRO	Money Laundering Reporting Officer
MONEVAL	Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MSBs	Money Services Businesses
OCC	Office of the Comptroller of the Currency – www.occ.gov
RBA	Risk Based Approach
Wolfsberg	A Group of 13 of the World's largest banks

Reference Sources

- Interpretive Note No 2 to Recommendation No 1. The FATF Recommendations – February 2012 – *www.fatf-gafi.org*

- The Australian Transaction Reports and Analysis Centre (AUSTRAC) website – *www.austrac.gov.au*

- AUSTRAC Annual Report 2014-15

- Australian Prudential and Regulatory Authority website – *www.apra.gov.au*

- FinCEN assessment of civil money penalty against Ocean Bank, Miami Florida - Number 2011-7

- FinCEN assessment of civil money penalty against Pamrapo Savings Bank S.L.A, Bayonne, New Jersey – Number 2010-3

- FATF Report – Money Laundering & Terrorist Financing Risk Assessment Strategies – June 2008

- FATF Report – Money Laundering through Money Remittance and Currency Exchange providers – June 2010

- FATF Money Laundering Using New Payment Methods – October 2010

- The Wolfsberg Group Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and bribery & Corruption - 2015

Exhibit A

Risk Management Policy and Strategy

A Schematic published by AUSTRAC