Guideline

Subject: **Deterring and Detecting Money Laundering and Terrorist Financing**

Category: **Sound Business and Financial Practices**

No: **B-8** **Date:** **December 2008**

INTRODUCTION

The fight against financial crime is an ongoing priority for governments around the world. The ability of criminals and criminal organizations to use financial institutions to launder funds, along with the potential risk to their reputations, and ultimately to their safety and soundness, continues to be a concern for financial and other regulators. Over the past several years there has been extensive action in many countries to implement permanent measures to fight money laundering and terrorist financing. This action has been driven largely by the leadership of the FATF, of which Canada is a founding member.

The FATF is the intergovernmental body that develops, monitors and evaluates country AML/ATF standards. These standards as set out in its 40 AML Recommendations and 9 ATF Recommendations establish a strong AML/ATF framework and permit a risk-based approach to the implementation of preventative measures.

The Government of Canada, led by the Department of Finance, has established a private/public sector advisory committee to gather information, on an ongoing basis, on how Canada's AML/ATF regime can be continuously reviewed. The federal Government also implemented significant changes to the PCMLTFA and PCMLTFR in 2007/2008 to ensure that the AML/ATF legislative framework is in line with international standards.

OSFI's mandate includes supervising financial soundness and promoting the adoption of policies and procedures designed to mitigate risk. OSFI believes that the risk management outcomes identified in this Guideline will further reduce the susceptibility of FRFIs to being used by individuals or organizations to launder funds and fight terrorist financing, thereby reducing their exposure to damage to their reputation, a key asset in the financial services industry.

To the extent possible, OSFI has aligned this Guideline to the framework of AML/ATF preventative measures set out in the FATF Recommendations. OSFI believes this will help focus attention on the principal goals of risk-based deterrence and detection.

Table of Contents

Compliance with this Guideline

FINTRAC is responsible for ensuring compliance with Part 1 of the PCMLTFA, and the PCMLTFR. These prescribe a compliance program with a risk-based component designed to ensure effective control over ML and TF risks.

This Guideline does not create any new regulatory requirements. It is intended to assist FRFIs in identifying and complying with applicable AML/ATF requirements and measures contained in the PCMLTFA and the PCMLTFR. This Guideline is also aimed at helping institutions meet OSFI's governance and control expectations.

Effective control over ML and TF risks, and related regulatory, operational and reputation risks, is essential.

In order to achieve effective control, FRFIs will adopt different approaches to their AML/ATF programs that take into account the nature, scope, complexity and risk profile of their institution. FRFIs are expected to take into account the contents of this Guideline when implementing their AML/ATF programs. OSFI's AML/ATF assessment program, which aims to assist OSFI in evaluating the effectiveness of controls, takes the foregoing into consideration in the assessment of individual institutions.

The OSFI Act enables OSFI and FINTRAC to exchange information on FRFIs' compliance with Part 1 of the PCMLTFA. To this end, on June 14, 2004, OSFI and FINTRAC signed a Memorandum of Understanding for exchanging information. FRFIs should also be aware that in December 2008, FINTRAC will be able to impose administrative monetary penalties against its reporting entities, including FRFIs, for violations of prescribed provisions of the PCMLTFA and PCMLTFR.

FRFIs should note that FINTRAC, as the agency responsible for ensuring compliance with Part 1 of the PCMLTFA, and the PCMLTFR, publishes and maintains its own Guidelines on compliance with the PCMLTFA and the PCMLTFR. OSFI has made every effort not to duplicate in substance FINTRAC guidance. This Guideline should therefore be read in conjunction with FINTRAC's Guidelines, as appropriate. Where we do refer to matters touched on in FINTRAC's Guidelines, we have conformed references to those used by FINTRAC.

"Fit & Proper" requirements for significant owners, directors and senior officers of FRFIs

The FATF Recommendations include measures to mitigate the risk that criminals and other inappropriate persons might take over ownership of, or unduly influence the management of, financial institutions.

OSFI screens all persons who own or control, directly or indirectly, significant interests in FRFIs. This screening is done prior to the approval of a new FRFI and when ownership interests change. In addition, OSFI screens directors and senior officers who will be in place when a FRFI commences operations. However, OSFI seeks to rely on FRFIs' internal processes for assessing

the ongoing suitability and integrity of directors and senior officers who are appointed after the FRFI's initial start up.

OSFI's expectations of FRFIs' internal processes for screening directors and senior officers post-authorization are set out in OSFI Guideline E-17 "Background Checks on Directors and Senior Management of FREs". A risk-based approach to assessing the FRFI's own screening processes is applied by OSFI where warranted. Compliance with Guideline E-17 in pertinent respects will be included in OSFI's AML/ATF assessment methodology.

Guidance on Designated Name Searching and Sanctions

Certain provisions of the PCMLTFA and the *Criminal Code* give both FINTRAC and OSFI responsibility for dealing with issues related to the financing of terrorist activities.

FINTRAC's objectives include the prevention, detection, and deterrence of the financing of terrorist activities, while OSFI's role is that of a central reporting channel for the aggregate reporting requirements outlined in subsection 83.11(2) of the *Criminal Code.*

With respect to FRFIs' terrorist property reporting obligations, OSFI posts on its Internet site (www.osfi-bsif.gc.ca) lists of terrorist individuals and organizations, and will continue to receive monthly reports from FRFIs on the findings of their continuous searching for and freezing of terrorist assets as required by the regulations under the *United Nations Act* or by subsection 83.11(1) of the *Criminal Code* in respect of designated entities. In addition, FINTRAC and a number of international organisations have published information related to terrorist financing activities. FINTRAC has also issued a guideline on Submitting Terrorist Property Reports.

Over the past few years, Canada has implemented several new economic and anti-proliferation (of weapons of mass destruction) sanctions against a number of countries, entities and designated persons. In addition, the FATF has issued guidance documents on a number of these and related matters. The array of obligations imposed on FRFIs by the reporting requirements, sanctions and related procedural actions merits dealing with designated name searching, listings, reporting, economic and anti- proliferation sanctions in a separate Guideline. OSFI anticipates that this Guideline will be issued in 2009[1].

Legislative Compliance Management

The components of the FRFI's AML/ATF program that are designed to comply with the PCMLTFA and PCMLTFR should be incorporated into, or referenced by, the FRFI's LCM framework. Although the chief compliance officer is responsible for the LCM framework generally (Guideline E-13: Legislative Compliance Management), the AML/ATF components of the LCM framework should be the responsibility of the CAMLO.

[1] In June 2010, OSFI issued an instruction guide on *Designated Persons Listings and Sanctions Laws*.

AML/ATF Guidance Issued by FATF and International Supervisory Bodies

The FATF, the Basel Committee on Banking Supervision and the International Association of Insurance Supervisors have each issued risk-based AML/ATF guidance directed at the financial sector. FRFIs should consult the appropriate guidance issued by these bodies for more information on risk assessment and effective controls.

THE RISK BASED APPROACH IN THE CONTEXT OF THE PCMLTFA AND PCMLTFR

The basic principle underpinning OSFI's *Supervisory Framework* is that FRFIs must develop and implement effective risk management controls to manage their exposure to financial risk and ultimately their financial stability and soundness.

This Guideline aims to assist FRFIs in their development and implementation of effective AML/ATF controls to manage their exposure to ML and TF risks.

The PCMLTFA and PCMLTFR prescribe various outcomes that FRFIs must achieve to detect and deter ML and TF. These outcomes are set out as regulatory requirements which, in the aggregate, form the compliance regime to be embedded in FRFIs' AML/ATF programs. Examples of regulatory requirements include: the identification of clients; the appointment of a CAMLO; determining whether a client is a PEFP; the prohibition on dealing with shell banks. Some requirements feed into broader outcomes; others are themselves outcomes.

In all cases, the manner in which these outcomes may be achieved is prescribed. Generally, there are three ways in which the PCMLTFA and the Regulations prescribe how an outcome is to be achieved:

1. By one or more Prescriptive Measures

In these situations, one or more measures are prescribed. All of the prescribed measures must be followed. An example is PEFP determination - if a client is determined to be a PEFP, certain prescribed measures must be taken.

2. By a choice of Prescriptive Measures

In these situations, a choice of alternative measures is prescribed. These measures offer FRFIs flexibility in achieving the prescribed outcome. Aside from selecting which option to choose, no other options or alternatives are available to the FRFI. Examples include prescribed types of acceptable identification documentation for individuals and prescribed sets of alternative measures for the identification of credit card clients in non-face-to face situations.

3. By Reasonable measures

In these situations, the PCMLTFA and PCMLTFR allow FRFIs more flexibility to determine for themselves how to achieve the prescribed outcomes, provided that the measures chosen are "reasonable". To be reasonable, the measures used must achieve the prescribed outcome. An example is reasonable measures to determine the source of funds for certain high risk clients.

This Guideline identifies measures that OSFI has found to be reasonable when applied effectively – i.e., when they achieve prescribed outcomes. The measures, which are drawn from a wide base of sources, including the FATF, should not be treated as checklists**.**

As noted below, OSFI expects FRFIs to have AML/ATF programs in place that include measures which are not expressly addressed by the PCMLTFA and PCMLTFR, but which are consistent with other OSFI Guidance and OSFI's Supervisory Framework.

AML/ATF PROGRAM

The AML/ATF program is the key vehicle for establishing and maintaining effective control over ML and TF risks in all relevant areas of the FRFI enterprise.

The following is a more detailed description of OSFI's expectations and prescribed content of the AML/ATF program:

Principal Elements of AML/ATF Program

FRFIs should ensure that their AML/ATF programs include the following elements, each of which is expanded upon in this Guideline. Elements required by the PCMLTFA and the PCMLTFR are marked with an asterisk:

- Senior Management Oversight, including *Reporting to Senior Management[2];
- *An appropriate individual responsible for implementation of the program[3]. See further, "CAMLO";
- *Assessment of inherent ML and TF risks[4]. See further, "Assessment of Inherent Risks";
- *Written AML/ATF policies and procedures that are kept up to date[5]. See further, "Control Policies and Procedures";
- *Written ongoing training program[6]. See further, "Ongoing Training";

[2] PCMLTFR ss. 71(2)
[3] PCMLTFR p. 71(1) (a)
[4] PCMLTFA ss. 9.6(2)
[5] PCMLTFR p. 71(1)(b)
[6] PCMLTFR p. 71(1)(d)

- Self Assessment of controls. See further, "Self Assessment of Controls"; and
- *Effectiveness testing[7]. See further, "Effectiveness Testing".

Scope

The AML/ATF program should implement a corporate standard of inherent risk assessment and risk control measures, across all relevant business areas of the FRFI.

The formality and sophistication of the AML/ATF program should be commensurate with the size and complexity of the FRFI and its businesses. As a general principle, the corporate standard should be consistent with Canadian regulatory requirements[8]. The PCMLTFA[9] requires that standards consistent with s. 6, 6.1 and 9.6 of the PCMLTFA be applied in respect of wholly owned subsidiaries and branches in countries that are not members of the FATF where the laws of such countries permit it. FRFIs should ensure that unless there is an explicit prohibition, such standards are applied.

FRFIs should notify OSFI if a country explicitly prohibits compliance with s. 9.7 or 9.8 of the PCMLTFA, to assist OSFI in analysing the situation in respect of that country.

SENIOR MANAGEMENT OVERSIGHT

Senior Management should have responsibility and accountability for: directing day-to-day implementation and management of the AML/ATF program; ensuring that it is adequate to mitigate ML and TF risk; that it complies with the PCMLTFA and PCMLTFR as required; and that it is implemented effectively in all relevant business areas.

Senior Management should ensure that:

- The CAMLO is appropriately qualified and has clear and documented authority and accountability for the design of the AML/ATF program;
- The CAMLO does not report to the Auditor or revenue-producing businesses, in order to avoid potential conflicts of responsibilities. In smaller FRFIs, where functional segregation may be difficult to achieve, compensating controls should be established to meet this goal. Consideration should be given to outsourcing the CAMLO function if compensating controls are not practical or possible**.**
- Qualified individuals have clear and documented responsibility and accountability for AML/ATF program implementation in all relevant business areas of operation, and sufficient resources to manage program implementation effectively;

[7] PCMLTFR p. 71(1)(e)
[8] PCMLTFA s. 6, 6.1 and 9.6
[9] PCMLTFA ss. 9.7(1) and s. 9.8

- The CAMLO and the Auditor have adequate resources in terms of people, data management systems and budget to implement and administer the AML/ATF program requirements effectively and to offer objective opinions or advice to Senior Management;
- All significant recommendations in respect of AML/ATF program issues and controls made by the CAMLO, the Auditor and Senior Management are acted upon in a timely manner.

Reporting

Senior Management should ensure they receive sufficient pertinent information from the CAMLO, the Auditor and other sources as appropriate, to enable them to ensure the overall adequacy and effectiveness of the AML/ATF program.

The PCMLTFR[10] prescribe timing and content of written reports on effectiveness testing, including reporting on any updates made to AML/ATF policies and procedures and the status of the implementation of such updates.

In larger, more complex, FRFIs, AML/ATF reports on effectiveness testing made at different times (for example, during audits of different business areas) should be collated and consolidated periodically. This will support the goal of assessing overall adequacy and effectiveness.

FRFIs should ensure that AML/ATF reporting to Senior Management by the CAMLO and by the Auditor is not unduly commingled, in order to differentiate the contents and purpose of the reporting.

The reports from the CAMLO should include information about: the FRFI-wide scope of the assessment of inherent risks including: significant patterns or trends; the self assessment of controls and material changes thereto; and remedial action plans or recommendations, if any, with milestones and target dates for completion. Where appropriate, the CAMLO should draw conclusions, offer advice or make recommendations about the overall structure and scope of the AML/ATF program.

Please refer to OSFI's *Corporate Governance Guideline* for OSFI's expectations of FRFI Boards of Directors in regards to operational, business, risk and crisis management policies.

CAMLO

Introduction

Whether or not the broader risk management structure of the FRFI is decentralized, responsibility for implementation of the enterprise AML/ATF program should be assigned to the

[10] ss. 71(2)

CAMLO, who should be one person positioned centrally at an appropriate senior corporate level of the FRFI. For the purposes of this Guideline, FRFIs should treat the CAMLO as an independent oversight function as described in OSFI's Corporate Governance Guideline.

The CAMLO is expected to be responsible both for the regulatory compliance component and the broader prudential risk management component of the AML/ATF program.

Mandate

FRFIs should ensure that the CAMLO has clear and documented responsibility and accountability for AML/ATF program content, design and enterprise-wide implementation. In particular, the CAMLO's mandate should include accountability for:

- oversight of AML/ATF control activity in all relevant business areas for the purposes of establishing a reasonable threshold level of control consistency throughout the enterprise;
- keeping the AML/ATF program current relative to the FRFI's identified inherent risks (clients and business relationships, products and delivery channels, geographic locations of activity and any other relevant factors);
- developing and implementing an assessment of inherent ML and TF risks, including but without prejudicing the generality of the foregoing, being satisfied that new product/service/business acquisition processes are subjected to timely inherent risk analysis and appropriate measures are developed to control identified risks. See further, "Assessment of Inherent Risks";
- being satisfied that systems resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are sufficient in all relevant areas of the FRFI;
- developing and implementing a self assessment of controls; see further, "Self Assessment of Controls";
- written AML/ATF policies and procedures that are kept up to date and approved by a senior officer;
- written ongoing training programs for Senior Management, employees, agents and other persons authorized to act on the FRFI's behalf;
- ensuring that the Auditor is aware of the requirement in the PCMLTFR for effectiveness testing of the AML/ATF program at least every two years;
- being satisfied that systems and other processes that generate information used in reports to Senior Management are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information; and
- reporting to Senior Management pertinent information about AML/ATF program adequacy and issues.

If the CAMLO delegates or assigns duties to other individuals, or if the FRFI assigns some elements of the AML/ATF program to business areas that do not report to the CAMLO, the

CAMLO should take reasonable measures to be satisfied that such elements are implemented satisfactorily. Reasonable measures to achieve this could include:

- where those responsible for filing STRs do not report to the CAMLO, being satisfied that threshold-based criteria are consistent, that reporting is accurate and timely, and ensuring the CAMLO receives regular summary reports on STR filings from such areas of the FRFI; and
- Establishing a management committee to coordinate the implementation of the AML/ATF program.

FRFIs should ensure that the CAMLO has:

- unfettered access to, and direct communications with, Senior Management and the Board; and
- unfettered access to all pertinent information, records and personnel throughout the FRFI.

Qualifications

Responsibility for the implementation of the AML/ATF program requires that the CAMLO have a thorough working knowledge of ML/TF risks and controls in the FRFI and AML/ATF regulatory requirements; a broad knowledge of the operations of the FRFI; and appropriate professional qualifications, experience and strong leadership skills.

Consideration should be given to these factors when FRFIs consider the seniority and reporting relationship of the CAMLO.

ASSESSMENT OF INHERENT RISKS

The PCMLTFA[11] requires that the compliance program include the development and application of policies and procedures to assess, in the course of a FRFI's activities, the risk of a ML or a TF offence.

The PCMLTFR[12] requires that the following categories of ML and TF risk be covered in a FRFI's assessment of inherent risk:

i. the clients and business relationships of the FRFI;
ii. the products and delivery channels of the FRFI;
iii. the geographic location of the activities of the FRFI; and
iv. any other relevant factor.

[11] PCMLTFA ss. 9.6(2)
[12] PCMLTFR p. 71(1)(c)

For the purposes of item (iv) above, FRFIs should take into account transaction risk factors, for example, structured or otherwise complex transactions, and factors that may fall into more than one of the other three categories.

Assessment of inherent risks refers to a process that:

- identifies current and emerging ML and TF risks inherent in activities of the FRFI without reference to any controls over them and whether or not the activities in which they reside are considered material in dollar terms;
- assesses the relative seriousness of the identified risks; and
- highlights the higher risks among them.

In considering ML and TF risks, consideration should be given to what, if any, pertinent changes have occurred since the assessment of inherent risks was last performed. Reasonable measures to accomplish this could include:

- consideration of factors that led to the filing of suspicious transaction reports and any patterns or trends in these; and
- consideration of external factors such as regulatory developments, ML or TF typologies and regulatory Notices and Advisories.

Regular assessment of inherent ML and TF risks enables FRFIs to tailor or adjust corporate control measures to identified risk, which in turn facilitates the allocation of more risk management resources to areas of greater vulnerability. See further, "Self Assessment of Controls" below.

The following sections discuss the methodology and desired outcomes of the process used to analyse inherent ML and TF risks.

Methodology

There is no single prescribed or universally used methodology for inherent ML/TF risk assessment. However, the methodology used should assess the risk of ML offences or TF offences across the FRFI and include the categories of risk identified in p. 71(1)(c) of the PCMLTFR.

The outcome of the methodology should be a rational, well-organized and well-documented inherent risk analysis.

Reasonable measures to include in the methodology used would include consideration of:

- the business lines and other operations of the FRFI;
- cross-border and international operations, if any, and linkages among these;
- typologies of how financial institutions have been abused; and
- any other relevant information that is available to the FRFI.

Risk Categories

Inherent risk assessment should address the different categories of risk exposure to ML and TF. The PCMLTFR[13] requires that inherent risk assessment address the following specific categories of risk. In each category, OSFI has indicated types of risks.

Client Risk:

This is risk associated with types of clients that buy or use the FRFI's products and services. Categories of clients that may indicate a higher risk could include:

- politically exposed persons;
- clients conducting their business relationship or transactions in unusual circumstances, such as geographic distance from the FRFI for which there is no reasonable explanation;
- clients whose nature, structure or relationship make it difficult to identify the ultimate beneficial owner(s) of significant or controlling interests, including clients that are corporations with the ability to issue bearer shares;
- cash (and cash equivalent) intensive businesses including:
    - Money services businesses (for example, remittance houses, foreign exchange businesses, money transfer agents, bank note traders, cash couriers or other businesses offering money transfer or movement facilities);
    - Casinos, betting and other gaming-related businesses;
    - Businesses that, while not normally cash-intensive, generate substantial amounts of cash for certain lines of activity; and
- charities and other non-profit organizations that are not monitored or supervised (for example, not registered with CRA).

Business relationship risk:

This is risk associated with the client's stated purpose in dealing with the FRFI. Categories of business relationships that may indicate a higher risk could include:

- intermediary structures, such as holding companies, numbered companies or trusts, that have no apparent business purpose or that make beneficial owners difficult to identify;
- accountants, lawyers or other professionals holding commingled funds accounts where the beneficial ownership of the funds may be difficult to verify; and
- use of the FRFI's products or services by clients of clients, for example, clients of correspondent banks.

[13] PCMLTFR p. 71(1)(c)

Product/Service Risk:

This is risk associated with FRFI products/services that enable clients to move funds. Categories of products and services that may indicate a higher risk could include:

- deposit-taking, especially cash, and insurance products that allow large one-time or regular payments, pre-payments or deposits, to be made and subsequently withdrawn from deposit or deposit-like accounts (for example, side accounts);
- "free look" or "cooling off" periods coupled with premium refunds, for example, in some life insurance products;
- cash values, early cash surrender and loan provisions, and provisions for deposit, accumulation and withdrawal of funds with relative ease and speed, for example, non-registered segregated funds;
- trade finance services where
    - the FRFI is not able to assess whether the values of goods or services being imported or exported are reasonable; or
    - FRFIs confirm, advise or make payments under letters of credit for purposes of their clients' buying or selling goods internationally.
- credit accounts in respect of which large credit balances are allowed to be maintained, for example, some credit and corporate card products;
- payable through accounts that permit clients of a foreign correspondent bank to draw drafts (or cheques) on Canadian-based accounts;
- lock boxes for the use of clients of foreign correspondent banks that permit such banks to collect payments due from their clients domiciled in Canada; and
- pouch services and similar international commercial payment services.

Delivery Channel Risk:

This is risk associated with how FRFIs' products/services are delivered to clients including services delivered to clients non-face-to-face. Categories of delivery channels that may indicate a higher risk could include:

- use of intermediaries or introducers (for example, mortgage and deposit agents and brokers), that may not be subject to AML/ATF laws and measures and who are not adequately supervised;
- the Internet, telephone and mail when used as a complete substitute for face to face interaction with the client in delivering banking services; and
- transfers payable upon presentation of identity (PUPIDs).

Geographic location risk:

This is risk associated with places in which FRFI activities are carried out. Where FRFIs have subsidiaries or branches in such places, this may mitigate or elevate the risk. Categories of countries that indicate a higher risk include countries:

- subject to Canadian or other national sanctions, embargoes or similar measures, such as the *Special Economic Measures Act* or measures prescribed under the USA PATRIOT Act;
- subject to United Nations Security Council (UNSC) sanctions (in Canada, UNSC sanctions are applied by regulations issued under the *United Nations Act*);
- identified by credible sources as providing funding or support for terrorist activities or the proliferation of weapons of mass destruction;
- identified by credible sources as having significant levels of corruption or other criminal activity;
- that are not members of the FATF, and in particular, countries that are subject to monitoring by the FATF or otherwise identified by the FATF as lacking appropriate AML/ATF regulatory requirements; and
- where legislation prohibits or unduly restricts access to client information by the CAMLO.

Other relevant factors:

FRFIs should ensure that they take any other relevant factors into consideration in an inherent risk assessment, including transaction risk factors and combinations of factors that may fall within more than one of the other three categories.

Rating and Ranking

An appropriate methodology should assign appropriate ML and TF risk levels to the pertinent activities of the FRFI and in so doing, identify the higher risks to which enhanced due diligence and ongoing monitoring must be applied.

The criteria used for rating and ranking should have a rational basis in ML and TF risk and address ML and TF risk factors that are unique to specific business lines, areas and jurisdictions, and also more general risk factors.

Finally, the methodology should enable FRFIs to comply with the regulatory requirement to identify higher risk clients activity[14] for purposes of establishing a threshold level of enhanced due diligence that is appropriate in the circumstances. See "Customer Due Diligence" below.

[14] PCMLTFA ss. 9.6(3)

Using Assessment of Inherent Risks as the Basis for Risk Controls

Results of the assessment of inherent risks should inform the development of risk controls, and the allocation of resources, commensurate with levels of ML and TF risk in the enterprise.

Certain risk control measures are prescribed by regulatory requirements. These cannot be qualified or bypassed by inherent risk assessments. They include, for example:

- client identification and ascertaining identity (subject to prescribed exemptions);
- determining under prescribed circumstances whether a client is a PEFP or is acting on behalf of a third party;
- reporting suspicious transactions and suspicious attempted transactions, large cash transactions and large EFTs; and
- record keeping.

CONTROL POLICIES AND PROCEDURES

Control policies and procedures should identify and implement measures designed to control inherent risks.

FRFIs should ensure that control policies and procedures are kept up to date to mitigate risks. They must also comply with other regulatory requirements: for example, the PCMLTFR[15] requires that written compliance policies and procedures form part of the AML/ATF compliance program and be approved by a senior officer.

Control policies and procedures should be embedded in business areas commensurate with the risks they are intended to mitigate, and otherwise tailored to the particular circumstances in which they operate.

Policies

AML/ATF policies should set risk management standards to govern the approach of the FRFI to deterring and detecting ML and TF, and should ensure regulatory compliance.

Policies setting a corporate standard should be approved by Senior Management and implemented consistently across the enterprise. They should establish clear and definitive requirements throughout the organization.

In keeping with the general principle that the corporate standard should be consistent with Canadian regulatory requirements (see "Policies" above), policies should implement the corporate standard, at least, of AML/ATF program requirements in wholly owned subsidiaries

[15] PCMLTFR p. 71(1)(b)

and branches outside Canada to the extent that laws of the foreign jurisdictions permit it. Policies should also reflect that unless there is an explicit prohibition, the corporate standard, at least, should be applied.

It should be noted that differences in local market conditions are not a sound basis for lowering or eliminating enterprise standards. In such cases, FRFIs should ensure that a specific risk assessment is made to determine whether operating in such markets would result in an unacceptable ML or TF risk to the FRFI.

Examples of topics that should be covered by policies are:

- what money laundering is. FRFIs should ensure that their policies and procedures adequately address their exposure to the stages of money laundering (placement, layering and integration) and are not unduly limited to anti-placement measures (for example, prohibitions or restrictions on the acceptance of cash);
- objectives of the AML/ATF program;
- key areas of inherent risk;
- Client due diligence standards reflecting:
    - minimum acceptable client identification requirements, verification standards, information gathering and monitoring;
    - prohibition on entering client relationships or processing transactions if identity cannot be ascertained;
    - appropriate or prescribed restrictions on entering client relationships or processing transactions before identity is established; the types of clients considered higher risk or not acceptable;
    - a definition of enhanced due diligence applicable to such higher risk clients; reporting; and
    - records retention;
- dealing with clients who exhibit levels of risk that are unacceptable to a FRFI;
- identification of clients whose accounts were opened prior to the coming into effect of the 2002 regulatory requirements and the PCMLTFR, and who have not been identified in accordance with the PCMLTFR, if such clients or their activities are assessed as being high risk[16];
- business rules defining what are unusual transactions and which unusual transactions are suspicious; and
- the mandates of key risk management control functions such as the Board, Senior Management, the CAMLO, the Auditor, and others.

[16] PCMLTFA ss. 9.6(3) and PCMLTFR p. 71.1(a)

Procedures

Procedures are the tools FRFIs use to translate AML/ATF policies into practice. Therefore, it is essential that procedures state clearly what actions are to be taken, by whom, where and when (noting pertinent regulatory deadlines as appropriate).

The evolving nature of AML/ATF regulation and changes to a FRFI's business require that procedures be updated on a regular basis to ensure their continued effectiveness. Should a FRFI's procedures allow for permitted exceptions, the procedures should include authorization processes and associated enforcement mechanisms to oversee such exceptions.

CLIENT DUE DILIGENCE (CDD)

CDD is comprised of client identification, information gathering, ascertaining identity and ongoing monitoring. These components must comply with applicable regulatory requirements, and must be enhanced for higher risk situations[17]. The extent of CDD performed should correspond to the relative level of assessed ML and TF risks in the circumstances. See "Specific Higher Risks" below.

As a general principle, a business relationship should only be entered into or maintained with a client if the FRFI is satisfied that the information it has gathered demonstrates that the FRFI knows the client (i.e. the client has disclosed his or her true identity and a legitimate purpose for entering or maintaining the business relationship with the FRFI). DTIs are required to keep a record of the intended use of each account opened, other than a credit card account[18].

The prescribed rules comprising CDD requirements do not permit FRFIs to establish anonymous[19] accounts for clients. If FRFIs provide services (such as account numbering or coding services) that effectively shield the identity of a client for business reasons (for instance, in a corporate acquisition where the premature circulation of information could jeopardize the transaction), or where client identity is withheld for proprietary reasons, FRFIs must ensure that they have appropriately ascertained the identity of the client and that this information is accessible by the CAMLO.

Where the regulatory requirements prescribe a determination of the status of a client, for example, the determination of whether a client is a PEFP, there must actually be a determination and FRFIs should ensure that a determination is made based on an assessment of the information received.

[17] PCMLTFR s. 71.1
[18] PCMLTFR p. 14(c.1)
[19] i.e., an account where the FRFI has not ascertained the identity of the client (other than certain products which are subject to specific identification exemptions under the PCMLTFR)

Nature and Amount

The nature and extent of CDD measures should be appropriate for the nature of, and proportional to the level of, the ML and TF risk that is posed by the client in the circumstances. See "Inherent Risk Assessment", above. At a minimum, CDD measures must comply with the requirements of the PCMLTFA and PCMLTFR. CDD standards should provide that where there are doubts[20] about the veracity or adequacy of previously obtained client identification and verification data, enhanced CDD must be performed.

FRFIs should enhance CDD measures if standard measures produce inconsistent, otherwise uncertain or doubtful results. The level of such enhanced due diligence should be sufficient to mitigate the inconsistencies, uncertain or doubtful results.

Client Identification and Ascertaining of Identity

FRFIs may have clients whose identities have not been ascertained in accordance with the PCMLTFR on account of having become clients prior to the AML/ATF requirements coming into force in 2002, or having purchased products that the PCMLTFR exempt from client identification requirements. FRFIs should ensure that if such clients subsequently purchase products to which client identification requirements apply, they are subject to appropriate client identification measures.

Reasonable measures to ensure that such clients are appropriately identified could include:

- ascertaining the identity of the client in respect of each product purchased; and
- establishing systems that flag otherwise unidentified clients who purchase products subject to prescribed client identification requirements.

The PCMLTFR specifies the originals of prescribed valid documents (or types of valid documents) that may be inspected to ascertain the identity of individuals and the existence of entities in face to face and non face to face scenarios, and the timing for doing so. A FRFI's CCD policy should provide clear direction that complies with the PCMLTFR, (where applicable) on:

- when a client's identity must be ascertained (timing);
- how to ascertain the identify of the client, when the client is present or not present; and
- which original and valid identification documents should be used to ascertain identification and what information is to be recorded from them.

While identification and verification standards and policies must meet the minimum prescribed requirements, FRFIs may consider that the assessment of inherent risk justifies the application of additional identification requirements to some categories of client.

[20] PCMLTFR ss. 63(1.1)

For example: the PCMLTFR[21] prescribes the use of valid government-issued documents to be used to ascertain the identity of a client. These include, *inter alia*, birth certificates. The PCMLTFR permits Social Insurance Number (SIN) cards to be used to ascertain the identity of a client. Where a birth certificate or a SIN card is the only document available to ascertain identity, and the assessed ML or TF risk of the client is other than minimal, FRFIs should consider applying additional identification measures. Such additional measures could include viewing the original of other acceptable government-issued identification documents, including government-issued photo identification, or, if these are not available, other credible evidence supporting the identity of the client such as a property tax or utility bill.

For persons without acceptable Canadian identification documents, comparable or equivalent foreign identification documents may be acceptable if they can be read and assessed as valid identification documents (for example, by reference to publicly available information) and can be understood by the FRFI.

Identifying a client that is a corporation or other entity may involve the collection of substantial information in some cases. In addition to confirming the existence of the entity[22], FRFIs must take reasonable measures to obtain the names and occupations of its directors and the names, addresses and occupations of individual(s) who are the ultimate beneficial owners of 25% or more of the entity[23]. Reasonable measures to obtain this information could include:

- requesting it from the entity;
- consulting a credible public or other database; or
- a combination of both.

Where a FRFI is required to obtain the occupation of a person (for example, a director of a client entity), the FRFI should ensure that the occupation obtained is the person's principal occupation and not merely the person's title in the client entity.

The measures applied should be commensurate with the level of assessed risk.

DTIs must also ascertain the identity of every person who signs a signature card in respect of a business account, except that where the signature card is signed by more than three authorized individuals, the identities of at least three of them must be ascertained[24]. The requirements of identification of individual clients are applicable. Life insurance companies should adopt a similar practice as a matter of prudent risk management because the inherent risk of not identifying signing officers for business accounts is similar.

[21] PCMLTFR ss. 64(1)
[22] PCMLTFR ss. 65(1)
[23] PCMLTFR s. 11.1
[24] PCMLTFR ss. 54(1)

The PCMLTFA and PCMLTFR prohibit FRFIs from opening accounts in prescribed circumstances if the FRFI cannot establish the identity of the client in accordance with prescribed measures[25].

FRFIs must also take reasonable measures, at times prescribed by the PCMLTFR[26], to determine whether the individual client is acting for or on behalf of a third party. Reasonable measures could include:

- asking the question on a product application; or
- including a negative assurance statement above the client's signature line on the application or other purchase document.

Life Insurance Companies

Life insurance companies are not required to ascertain the identity of, or obtain the identification information of, a person where there are reasonable grounds to believe that the person's identity has been ascertained in the prescribed manner by another life insurance company or life insurance broker or agent in respect of the same transaction or of a transaction that is part of a series of transactions that includes the original transaction[27]. For these situations, life insurance companies should therefore develop and implement policies and procedures designed to ensure that:

- they perform appropriate initial and ongoing due diligence on other life insurance companies, life insurance brokers or agents; and
- there are reasonable grounds to believe that the client identification and verification procedures used by such other life insurance companies, life insurance brokers or agents comply with the PCMLTFA and PCMLTFR and with the life insurance company's own policies and procedures.

OSFI understands that with respect to individual products, in practice life insurance companies do receive information about the identity of the client on application forms submitted by life insurance agents or brokers. This practice enables life insurance companies to periodically determine that the grounds for relying on such agents are reasonable.

Source of Accumulated Funds or Wealth

FRFIs should satisfy themselves that, in appropriate circumstances, the amount of clients' accumulated funds or wealth appears to be reasonable and consistent with the information provided. Doubts about the origin of such funds or wealth should be satisfied before proceeding

[25] PCMLTFA s. 9.2
[26] PCMLTFR ss. 9(1) DTIs; PCMLTFR ss. 10(1) life insurance companies; PCMLTFR ss. 8(1) large cash transactions
[27] PCMLTFR ss. 56(2)

with the relationship or permitting transactions to occur. Reasonable measures to implement this requirement could include:

- obtaining and evaluating more detailed information from the client; and
- verifying information obtained from other financial institutions or references.

Where doubts persist, consideration should be given to not proceeding with the relationship or transaction.

In cases where a client is assessed as higher risk **and** the source of accumulated funds or wealth does not appear to be reasonable, or is inconsistent with the information provided despite taking reasonable measures to resolve the inconsistency, the FRFI should consider declining to enter the business relationship, or terminating it, and consider filing a suspicious attempted transaction report.

Monitoring

Standard

FRFIs must be able to identify suspicious transactions, or suspicious attempted transactions, and report these to FINTRAC. Further, FRFIs must take reasonable measures to ascertain the identity of every person with whom the FRFI conducts a transaction that is determined by the FRFI to be suspicious[28]. These obligations imply that the activities of all clients, regardless of their risk ranking, must be subject to some form of ongoing monitoring to detect transactions or attempted transactions that are potentially suspicious.

Reasonable measures for such monitoring could include:

- Identification and review of types of transactions or attempted transactions (defined by size, frequency, geographical location, delivery channel, business relationship or other factors) that appear to be inconsistent with the intended purpose of the account or the circumstances; and
- Changes in transaction activity that may on their own or in conjunction with recorded changes in client information, be indicative of a change in the nature of a client's business or intended use of the account.

FRFIs should conduct feasibility studies, as appropriate, to determine whether transaction volumes merit the application of information technology solutions to transaction monitoring.

Monitoring should identify information, transactions or attempted transactions that are unusual or potentially suspicious and that require further analysis. Monitoring criteria should cover all relevant indicators. Relevant indicators could include:

[28] PCMLTFR s. 53.1

- frequent and unexplained movement of accounts to different financial institutions;
- frequent and unexplained movement of funds between different financial institutions in various geographic locations;
- client information about or explanations for the source of transaction funds or accumulated wealth that is not clearly reasonable or credible;
- transactions that are structured or otherwise complex, or unusually large relative to the size and business of the client or the geographical location of the transaction;
- types of transactions, or patterns of transactions, inconsistent with the purpose of the account or the business of the client; and
- transactions that have no apparent economic or visible lawful purpose.

Enhanced

The PCMLTFA and PCMLTFR provide that where a FRFI determines that the risk of a ML or TF offence is high, FRFIs must take prescribed special measures for identifying clients, keeping records and monitoring financial transactions in respect of the activities that pose the high risk[29]. The prescribed special measures include: reasonable measures to determine whether the high risk client is a PEFP[30]; keep client identification information and the information referred to in PCMLTFR s. 11.1 up to date[31]; conduct ongoing suspicious transaction and suspicious attempted transaction monitoring[32]; and generally mitigate the high risk[33].

FRFIs should consider creating more than one category of higher risk client, and more than one category of enhanced due diligence, if the nature, scope, complexity and risk profile of the financial institution merit such action. Each level of enhanced monitoring should reflect the assessed level of risk appropriately.

Reasonable measures for applying enhanced monitoring could include:

- More frequent reviews of client activity and types of activity;
- More frequent updates or reviews of client information;
- The application of additional client identification measures;
- The gathering of information from public or open sources such as commercial databases;
- More frequent flagging of unusual transactions or other information; and

[29] PCMLTFA ss. 9.6(3)
[30] PCMLTFR p. 54.2(b)
[31] PCMLTFR p. 71.1(a)
[32] PCMLTFR p. 71.1(b)
[33] PCMLTFR p. 71.1(c)

- Referral of client activity and transactions to a more senior officer in the FRFI for review.

Additional measures that could be taken to strengthen the monitoring of high risk activities include:

- Review of business reports, including exceptions reports, generated by management information systems (for example, anti-fraud systems), for possible indicators in them of unusual or suspicious activity.
- Analysis of STR information for trends and other indicators of suspicious activity to aid the development of appropriate risk-based controls in businesses that indicate such activity.

SPECIFIC HIGHER RISKS

This section discusses OSFI's expectations and prescribed measures in respect of enhanced due diligence and related controls applicable to areas of identified higher risk.

Use of Agents or Mandataries

Many FRFIs rely on introducers, intermediaries or other third parties[34] for client information gathering and verification purposes. These include, for example, deposit and mortgage brokers and solicitors. ML and TF risk mitigation can be compromised where FRFIs do not ensure that appropriate client identification standards are applied by the introducers, intermediaries or other third parties.

With one exception for life insurance companies referred to above, accountability for ascertaining the identity of the client and obtaining the information used to identify the client remains with the FRFI when it uses a third party to ascertain the identity of clients. In respect of this accountability, FRFIs must have an agreement or arrangement in writing with the agent or mandatary if such person is to be responsible for client identification and verification. The provisions of this arrangement or agreement must conform to the requirements of the PCMLTFR[35] and it should obligate the agent or mandatary to:

- apply the DTI's or life insurance company's client identification and verification requirements (which must comply with the regulatory requirements);
- ensure that, where the client is present at the time client identification is ascertained, the agent or mandatary applies client identification procedures that include viewing original identification documents;

[34] Referred to as "agents" or "mandataries" in s. 64.1 of the PCMLTFR
[35] PCMLTFR s. 64.1

- ensure that, where the client is not present at the time client identification is ascertained, the agent or mandatary applies prescribed non-face-to-face identification requirements[36]; and
- provide the client identification information to the DTI promptly after obtaining it.

DTIs and life insurance companies should also:

- ensure that if the agent or mandatary is responsible for collecting the information required to make a third party determination or a PEFP determination, these responsibilities are also documented;
- Ensure they receive client identification information in the required timeframes; and
- periodically review, in a systemic manner, the quality of client information gathered and documented by the agent or mandatary to ensure that it continues to meet their requirements.

Documentation of relationships and communications with, and client due diligence work of, agents and mandataries, should be complete and current, and client information should be placed in the client's record promptly upon receiving it. See further, "Record Keeping and Retention", below.

FRFIs should consider terminating relationships with agents or mandataries that do not comply with agreed upon client identification responsibilities or provide the DTI or life insurance company with the requisite client information on a timely basis.

Contracts with agents and mandataries should be reviewed and updated as necessary to ensure compliance with the PCMLTFR[37] regarding the use of agents and mandataries.

The extent of the DTI's or life insurance company's exposure to the agent or mandatary for the results of client due diligence should be addressed expressly in the DTI's or life insurance company's inherent risk assessment.

Fraud with respect to Mortgage Loans and other Products

Fraudulent misrepresentation in respect of FRFIs' products takes many forms that could include:

- Forged or falsified employment letters or references, or misrepresented self-employment;
- Forged or falsified pay stubs, T4 slips, and CRA Notices of Assessment;
- Forged or falsified personal identification documents;
- Use of "straw" (i.e., non-existent) individuals;
- False or falsified credit records;

[36] FINTRAC Guideline 6G, section 4.12
[37] PCMLTFR s. 64.1

- Concealed legal or beneficial ownership;
- Concealed sources of down payment; and
- Inflated assets.

FRFIs should ensure their client acceptance and due diligence processes address the risk of fraud, a predicate offence for money laundering. FRFIs should take reasonable measures to address the risk, which could include:

- Applying enhanced client identification measures such as viewing a second piece of identification, or viewing government-issued photo identification;
- Having an agent or mandatary apply enhanced non-face-to-face client identification measures;
- Ensuring that legal and/or beneficial ownership of property or business is understood and documented;
- Satisfying themselves that the amount of clients' accumulated funds or wealth appears to be reasonable and consistent with the information provided (see further, "Source of Accumulated Funds or Wealth" above);
- Training staff, agents or mandataries in the recognition of valid identification documents and signs of falsification of documents;
- Obtaining corroboration of information in employer letters, references, pay stubs or credit records, as appropriate; and
- Corroborating the existence and value of stated assets.

Life insurance companies should ensure that mortgage loans are subject to the AML/ATF program.

PEFPs

The FATF Recommendations state that PEPs are potentially more susceptible to financial crime than other clients of financial institutions. In Canada, the PCMLTFA requires FRFIs to determine, in prescribed circumstances, whether they are dealing with PEFPs and also prescribes mandatory enhanced due diligence measures to be taken in respect of PEFPs in prescribed circumstances.[38]

A PEFP is defined in the PCMLTFA as an individual who holds or has ever held prescribed offices or positions in or on behalf of a foreign state or is a prescribed member of the family of such a person[39].

[38] PCMLTFA s. 9.3
[39] PCMLTFA ss. 9.3(3)

For purposes of the foregoing, the term "foreign state" should be interpreted to include the principal political subdivisions of foreign countries when applying the PEFP definition.

Once the determination is made, prescribed actions must be taken within minimum time periods.

Timing of PEFP determination - DTIs

There are three situations that trigger the requirement for DTIs to determine whether a client is a PEFP:

- when an account is opened[40];
- when an existing client is deemed to be high risk[41]; and
- when a client initiates or receives an EFT of $100,000 or more[42].

The determination and approval by a senior officer to keep the account open must be made no later than 14 days from account activation[43] or within 14 days of the EFT being received or sent[44]. There is no specific time period in respect of determination as a result of a risk assessment. FRFIs should ensure that the PEFP determination required when an existing account is deemed to be high risk is made no later than 14 days thereafter, to be consistent with other prescribed requirements.

Timing of PEFP determination – Life Insurance Companies

Life insurance companies must take reasonable measures to determine if a person who makes a lump-sum payment of $100,000 or more in relation to an immediate or deferred annuity or life insurance policy on their own behalf or on behalf of a third party is a PEFP[45]. Such person may not be the policy holder.

The determination must be made within 14 days of the payment transaction[46].

Points to Consider in Making a PEFP Determination

The PCMLTFA and PCMLTFR require that FRFIs take "reasonable measures" to make the PEFP determination. Reasonable measures could include:

- Asking the individual for information that could indicate PEFP status, such as existing or previous connections to the prescribed relationships;

40 PCMLTFR paragraph 54.2(a)
41 PCMLTFR paragraph 54.2(b)
42 PCMLTFR paragraph 54.2(c), (d)
43 PCMLTFR ss. 67.1(2)
44 PCMLTFR ss. 67.2(3)
45 PCMLTFR s. 56.1
46 PCMLTFR ss. 67.2(3)

- Screening the individual's name and other personal information against a commercially or publicly available database to gather more information about the individual; or
- a combination of both.

About asking the Client

If FRFIs choose to ask the individual for information, FRFIs should keep in mind that clients should not be expected to know the criteria that determine whether they are PEFPs. FRFIs should also note that there is no obligation imposed on FRFIs to disclose to a client that a determination must be made, or needs to be made.

A reasonable approach would be to ask the client if the client has or has ever had a prescribed connection to a foreign state, government, military or judiciary. The questions could be expanded to cover family members with any similar connections. If the responses are not clear or inconclusive, additional assessment or due diligence may be necessary before finalizing the determination. The additional measures could range from asking the applicant for more information, to internet searches, to running the individual(s') name(s) against a public database.

FINTRAC has published a pamphlet that FRFIs can use to explain to their clients, if necessary, why they need to enquire about their background. This pamphlet can be viewed at FINTRAC's Internet site.

About consulting a commercial database

FRFIs that choose to screen names and other personal information against a commercial or publicly available database should ensure they:

- Determine whether the provider identifies in the database individuals who fit the definition of PEFPs in the PCMLFTA and PCMLTFR. Most of these databases are built using open source (i.e. public) information. If the family members of a PEFP are not well known, there is no guarantee that a database will know about them.
- Establish the frequency and methodology used to update the information in the database, including whether the provider removes names from the database when officeholders leave office or die. If names are removed, the database may not capture persons who "have ever been" PEFPs.
- Establish a process to discard false positive hits, and identify other steps to be taken if the information in the database is inconclusive.
- Are able to screen the names of clients in all business lines against this list, especially if the FRFI has manual procedures, legacy systems, or uses the database to screen for the names of designated persons under anti-terrorist regulations.

OSFI does not expect FRFIs to depend on a client database in making a PEFP determination where the information obtained from the client shows that the client is a PEFP. Clients, who initially provide information that clearly establishes them to be PEFPs, must be determined to be

PEFPs and need not be scrubbed through databases unless it is done merely to obtain background or additional information.

Refer to the discussion about “reasonable measures” in "Client Due Diligence", above. FRFIs should ensure a determination is made based on an evaluation of the information received from a client or a database.

FRFIs should also ensure that, where a client is determined to be a PEFP, and the FRFI is aware that the client has family members who are also PEFPs by reason of the definition in the PCMLTFA, the names of such family members are scrubbed against the FRFI’s client databases to determine if accounts are held in such names by the FRFI.

FRFIs that use agents or mandataries (deposit brokers, mortgage brokers or others) to identify their clients and remit client identification information to them retain responsibility for PEFP determination. FRFIs may assign responsibility for collecting the information necessary for the FRFI to determine if the client is a PEFP, but the FRFI, not the agent, is responsible for making the determination and for applying the prescribed measures accordingly. FRFIs should ensure that where agents or mandataries are responsible for gathering the information, the agents understand what is required to be done and the FRFI satisfies itself that its agents are doing what is required.

If a client’s name is contained in a public database, but the FRFI does not determine the client is a PEFP, the FRFI may wish to make a note of the “hit” for future reference or to guide it in any future risk assessment.

What Happens after a PEFP Determination is made

Once a PEFP determination is made, it may not be reversed or otherwise changed, other than to correct error. The PEFP definition provides that the criterion or criteria that trigger PEFP status remain(s) in effect in perpetuity.

When a client is determined to be a PEFP a FRFI must:

- Take reasonable measures to establish the source (i.e., how the client acquired the funds in the account) of the PEFP’s funds; see “Applying PEFP Determination to Canadian sources of funds or payments”, below;
- For DTIs, obtain the approval of a senior officer to keep the account open; for life insurance companies, ensure that a senior officer reviews the transaction; and
- Conduct enhanced ongoing monitoring of the PEFP’s account to identify potentially suspicious transactions.

Reasonable measures to establish source(s) of funds include asking the client to explain how the client came to hold the funds. Examples of source of funds could include: savings accumulated through employment; sale of investments; sale of a business; an inheritance; a salary bonus; and consulting fees.

In respect of the approval by a senior officer, such individual should be a person at a more senior level who has the authority to make this decision.

Reasonable measures for enhanced and ongoing monitoring of PEFPs' accounts may involve manual or automated processes, or a combination of both depending on resources and needs and could include:

- Developing reports or performing more frequent review of PEFP account activity, and flagging activities that deviate from expectations and elevate concerns as necessary;
- Setting up a management committee to regularly review all identified PEFPs and their transactions; and
- Reviewing transactions more frequently against indicators of suspicious transactions.

PEFPs in Canada and Domestic PEPs

The PEFP definition in the PCMLTFA indicates that the country of residence or citizenship of an individual is immaterial to PEFP determination. FRFIs should therefore ensure that their methodology of PEFP determination does not preclude individuals merely because they may be Canadian citizens or residents.

FRFIs may need to ensure they distinguish between PEFPs and domestic PEPs. The latter are not separately defined in the PCMLTFA definition of PEFP, although a PEFP could also be a domestic PEP. However, FRFIs are not under any legal obligation to identify domestic PEPs *per se*, whether by screening or flagging large transactions or in any other way. Further, even if FRFIs know they are dealing with a domestic PEP, they are not under any legal obligation to apply the measures that are applicable to PEFP accounts, unless that individual is a PEFP.

Where a FRFI is aware that a client is a domestic PEP, the FRFI should assess what effect, if any, this may have on the overall assessed risk of the client. If the assessed risk is elevated, the FRFI should apply enhanced due diligence measures as it considers appropriate.

Identification of PEFPs in Foreign Subsidiaries or Branches

The PCMLTFA and PCMLTFR do not oblige FRFIs to apply PEFP measures to their subsidiaries or branches of FRFIs outside Canada.

Where a FRFI is aware that a client of a subsidiary or a branch outside Canada is a PEFP, the FRFI should assess what effect, if any, this may have on the overall assessed risk of the client. If the assessed risk is elevated, the FRFI should apply enhanced due diligence as it considers appropriate.

The operations of foreign branches and subsidiaries may be subject to local AML/ATF legislation, which may include requirements to identify and monitor PEPs, including PEFPs.

Identification of PEFPs who own or control 25% or more of Clients that are Corporations or Entities, or who are directors or officers of such corporations or entities

FRFIs are not obliged by the PCMLTFA or PCMLTFR to apply PEFP determination procedures to persons who own or control 25% or more of clients that are corporations or entities, or who are directors or officers of such corporations or entities.

Where a FRFI is aware that a person who owns or controls 25% or more of a client that is a corporation or entity, or who is a director or officer of such a corporation or entity, is a PEFP, the FRFI should assess what effect, if any, this may have on the overall assessed risk of the client corporation or entity. If the assessed risk is elevated, the FRFI should apply enhanced due diligence as it considers appropriate. Appropriate due diligence could include:

- A determination as to whether the PEFP is a client of the FRFI, and, if so, whether enhanced monitoring procedures should apply to the client's and the PEFP's transactions.
- Enhanced monitoring of the client account.

Applying PEFP determinations to Canadian sources of funds or payments

For life insurance companies**,** the PCMLTFR[47] does not distinguish between domestic and foreign payments. Accordingly, life insurance companies should apply a PEFP determination to prescribed funds from any source, domestic or foreign.

For DTIs**,** domestic transfers into or out of an account do not, of themselves, trigger any requirement to make a PEFP determination[48].

However, if a DTI has already determined that a client is a PEFP, OSFI believes that a risk assessment should be made to determine whether monitoring domestic incoming transfers would be advisable.

Client Corporations that can issue bearer shares

Identifying a client that is a corporation that can issue bearer shares may require special customer identification measures. Bearer shares can hide the identity of beneficial owners of the client corporation. If the aggregate of such shares could amount to more than 25% of such client corporation, a FRFI might be unable to identify the beneficial owner(s).

Where a FRFI assesses (using the risk categories outline above) that the risk of dealing with such a client corporation may be present, the FRFI should apply reasonable measures to mitigate this risk. Reasonable measures should always include obtaining the identity of the person or persons

[47] PCMLTFR s. 56.1
[48] PCMLTFR p. 54.2(c)

who beneficially own 25% or more of the shares of the corporation taking into account any issued and outstanding bearer shares, and could also include one or more of the following:

- Requesting the client corporation to immobilize any issued and outstanding bearer shares, for example, by arranging for the certificates representing such shares to be placed with a custodian such as a trustee. The arrangement should permit the FRFI to:
    - Verify on request that the shares continue to be held by the custodian; and
    - Be advised on a timely basis of any change in ownership of the shares that may change this information.
- Requesting the client corporation to amend its charter documents to remove the power to issue bearer shares and limit the issue of new shares;
- Requesting the client corporation to cancel any issued and outstanding bearer shares and replace them with shares in registered form.

FRFIs should ensure that the measures taken are documented.

Correspondent Banking

For the purpose of this Guideline, "correspondent banking relationship" has the same meaning as in the PCMLTFA.

Correspondent banking relationships are established between banks to facilitate, among other things, transactions between banks made on their own behalf; transactions on behalf of their clients; and making services available directly to clients of other banks. Examples of these services include: inter-bank deposit activities; international electronic funds transfers; cash management; cheque clearing and payment services; collections; payment for foreign exchange services; processing client payments (in either domestic or foreign currency); and payable-through accounts.

Correspondent banking relationships with foreign financial institutions (FFIs) are identified by the FATF as a specific higher risk area, and consequently the PCMLTFA and PCMLTFR prescribe measures[49] to be applied by FRFIs that enter into correspondent banking relationships with FFIs and their clients.

FRFIs that offer payable through accounts services to customers of FFIs must take reasonable measures to ascertain whether the FFIs have met requirements that oblige them to identify and ascertain the identities of such clients that are consistent with the requirements of the PCMLTFR, and ensure that the FFIs will provide relevant customer identification data to the FRFI, upon request[50]. Reasonable measures to achieve these requirements could include:

[49] PCMLTFA s. 9.4 and PCMLTFR s. 55.1, 55.2
[50] PCMLTFR s. 55.2

- Obtaining copies of the FFI's AML policies, and in particular its customer acceptance policies, and reviewing these for consistency with the requirements of the PCMLTFR;
- Ensuring that the documentation of the agreement with the FFI includes an obligation on the part of the FFI to provide relevant customer identification information to the FRFI when requested to do so.

Reasonable measures to monitor correspondent banking relationships generally could include, for example:

- Establish and periodically update an AML country risk rating system and assign a rating to each country in which a correspondent banking relationship has been established, for the purpose of implementing an appropriate level of monitoring;
- Review the FATF (or FATF style regional body's) mutual evaluation report or other assessment of the FFI's home country's measures to implement the FATF 40 Recommendations and 9 Special Recommendations;
- Review the FFI's ownership and background;
- Be satisfied that its activities are authorized, regulated and supervised by the relevant regulatory authority in its home country;
- Meet or otherwise communicate with senior representatives of the FFI to understand their commitment to effective control of ML and TF and understand key provisions of the FFI's AML/ATF policies and procedures such as those dealing with client acceptance; and
- Use the services of credible third parties (such as those providing a document repository or AML/ATF rankings) as a source of additional information on the FFI and its regulatory environment.

Where a FRFI ascertains, pursuant to s. 55.1 of the PCMLTFR, that there are civil or criminal sanctions imposed against a FFI in respect of AML/ATF requirements; or where a FRFI ascertains that a FFI does not have in place AML/ATF policies and procedures as specified in ss.15.1(3) of the PCMLTFA; then for the purpose of detecting any suspicious transactions required to be reported to FINTRAC under s. 7 of the PCMLTFA the FRFI should conduct ongoing monitoring of all transactions in the context of the correspondent banking relationship to mitigate the higher risk[51]. The extent of such monitoring in the case of sanctions identified against a FFI should correspond to the context, severity and type of sanctions imposed on the FFI. Reasonable measures could include:

- Reviewing in more depth the FFI's client acceptance process and its process for risk assessing its clients, products and services;
- Training officers of the FRFI on the required enhanced transaction monitoring requirements to be applied with respect to the relationship, including those transactions of the FFI's clients that are permitted to access the FRFI's banking services;

[51] PCMLTFR ss. 15.1(3)

- Escalating the level of Senior Management responsible for the relationship;
- Reviewing transactions over threshold amounts (using a risk-based approach), identified by analyzing client risk, business relationship risk, product/service risk, delivery channel risk, geographic risk and other relevant risk factors;
- Reviewing the FFI's methodology for monitoring and surveillance of transactions, in particular those that ultimately result in a transaction being processed by the DTI (e.g. an international wire payment, payment under a letter of credit, etc.) and preparing a summary of the key AML/ATF policies and procedures of the FFI as well as providing details on the due diligence carried out; and
- Conducting risk-based retrospective due diligence on existing clients utilizing the correspondent banking relationship using the FRFI's standards and criteria established in accordance with the PCMLTFA and PCMLTFR; and
- Giving consideration to restricting or discontinuing payable-through account services if the FRFI's analysis of the relationship concludes that the FFI's polices and procedures do not meet the standards set out in s. 55.2 of the PCMLTFR.

A FRFI acting as an intermediary bank may not be in a position to understand the purpose of EFTs originated by clients of FFIs or other originator banks, or conduct CDD on these persons. Consequently, such a FRFI that receives a cover payment for transactions may not be in a position to determine whether EFTs represented by the cover payment are suspicious, based on an understanding of the activities of the originator (and the beneficiary, if the beneficiary is not a client of the FRFI). It is, however, possible for intermediary FRFIs to monitor transactions that they process to identify patterns of activity that may be suspicious, to report suspicious transactions or attempted transactions, and, where such transactions are associated with a particular FFI, to review the relationship with that FFI.

Processing Electronic Funds Transfers

All information prescribed by the PCMLTFA and PCMLTFR, including originator information[52], must be included on all outgoing international EFTs and domestic SWIFT payments originated by FRFIs.

In addition, FRFIs must take reasonable measures to ensure that incoming EFTs include originator information. FRFIs that act as intermediary banks should develop and implement reasonable policies and procedures for monitoring payment message data subsequent to processing. Such measures should facilitate the detection of instances where required message fields are completed but the information is unclear, or where there is meaningless data in message fields. Reasonable measures could include:

- Contacting the originator's bank or precedent intermediary bank to clarify or complete the information received in the required fields;

[52] PCMLTFA p. 9.5(b)

- considering (in the case of repeated incidents involving the same correspondent or in cases where a correspondent declines to provide additional information) whether the relationship with the correspondent or the intermediary bank should be restricted or terminated; and/or
- filing a suspicious transaction report.

The reasons for decisions taken should be documented.

Trade Finance

Traditional trade finance services include letters of credit or other financial products, which give FRFIs the opportunity to view and assess details of the transaction that triggers an international payment.

FRFIs that outsource trade finance services to other financial institutions should ensure that this outsourcing is included in the FRFI's inherent risk assessment. If the assessment indicates that the risk of ML and TF is elevated, the FRFI should implement reasonable measures to control the risk. Reasonable measures could include:

- Conducting an analysis of the provider's policies and practices; and
- Communicating to the provider what AML/ATF control measures the FRFI expects the provider to have in place. The FRFI should have the right to audit such measures.

OSFI recognizes that FRFIs whose services are used to make trade finance payments on an open account basis may not have an opportunity to review the nature of a client's underlying trade transaction. Reasonable measures to address this risk could include:

- Periodic verification, using credible open source material or information, of the business of the client that triggers the need for such payments;
- Periodic review of electronic funds transfer data to determine whether the client's business includes significant trade activity;
- Periodic review of the client's transactions compared to the FRFI's record of the intended purpose of the account;
- Meeting or other interaction with the client; or
- Periodic confirmation that the client is not in a type of business to which the FRFI has decided, as a matter of policy, not to provide financial services.

Under- and over-Invoicing of Goods and Services

The FATF has advised[53] that the laundering of funds through under- and over-invoicing is one of the oldest methods of fraudulently transferring value across borders, and remains a common practice. The key element of the technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter. Many such cases have been identified by the FATF.

Multiple Invoicing of Goods and Services

By invoicing the same good or service more than once, a money launderer may be able to justify multiple payments for the same shipment of goods or delivery of services, especially if more than one financial institution is used. Multiple invoicing avoids the need to misrepresent prices.

Over- and Under-Shipments of Goods and Services

A third method of illicitly moving funds is to move more, less, or no goods.

Other and More Complex Trade-based Money Laundering Techniques

The foregoing techniques can be combined in more complex series of arrangements. For example, the so-called Black Market Peso Exchange is a known technique used to launder the proceeds of the sale of drugs. For more detailed information on techniques and typologies associated with this and other trade-based money laundering, FRFIs are requested to consult FATF material available on the FATF web site.

Assessing the Risks in Trade Finance Services, and Enhanced Measures to Mitigate Assessed Risk

Where the assessed risk of ML or TF in trade finance services is elevated, FRFIs should take reasonable measures designed to mitigate the risk of misuse of trade financing mechanisms. Reasonable measures could include:

- Conducting periodic on-site assessment of the risks posed by clients and the procedures they follow;
- Reviewing the routing of shipments and note ports of call or transhipment points that are inconsistent with a standard commercial transaction, for example, a shipment of steel from Canada to Asia routed via a European port or a country where there is no apparent business rationale for the routing, or where the routing or the carrier is located in a high risk country;

[53] Trade Based Money Laundering, 23 June, 2006, available on the FATF Web site.

- Subjecting requests involving letters of credit to cover shipments of goods that are not consistent with the applicant's normal business patterns to more detailed review and noting the results in the client's records;
- Identifying significant differences (either between different clients, different shipments or market quotes) in prices of a good or commodity being financed under a letter of credit, and determining the business rationale for the differences; and
- Making additional enquiries about the business rationale of transactions involving multiple banks and payments flowing through intermediaries as opposed to directly from the importer's bank to the exporter's bank.

New and Developing Technologies

Developments in technology frequently drive the creation of new financial products and services. Such developments can lower costs, improve client service and expand markets. FRFIs should have policies and procedures in place to ensure that new and developing technologies are included in the FRFI's inherent risk assessment process. In this way FRFIs can ensure that appropriate AML/ATF controls are in place, and, where appropriate, develop or amend controls to take new risks into account. Examples of new and developing technologies include stored value cards that may permit clients to subsequently download those funds directly into a deposit or a credit account and mobile telephone technology and various e-money services that have similar characteristics.

RECORD KEEPING AND RETENTION

Procedures for keeping paper and electronic records of pertinent information about clients and transactions must ensure that the FRFI complies with all of the record keeping requirements of the PCMLTFA and PCMLTFR. These include:

- for clients that are entities: prescribed information, if obtained, about beneficial owners of corporate clients and other prescribed information on corporations and other entities[54];
- for large cash transactions: large cash transaction records[55]; related client records[56];
- for account opening: prescribed information about client individuals and entities for non-credit card account opening[57]; and prescribed information about credit card holders for credit card account opening[58];
- for account operation: account operating agreements[59] and other prescribed information[60] for non-credit card accounts; and credit card account records for credit card accounts; [61];

[54] PCMLTFR ss. 11.1(1)
[55] PCMLTFR s. 13
[56] PCMLTFR p. 50(1)(c), ss. 50(3)
[57] PCMLTFR p. 14(a)-(c)
[58] PCMLTFR s. 14.1

- for credit transactions: new credit files[62];
- for currency exchange: foreign currency exchange transaction tickets[63];
- for transactions of $3,000 and more with non-account holders: prescribed information for traveller's cheques, money orders or similar negotiable instruments[64]
- for prescribed incoming EFTs: prescribed information[65];
- for trusts with respect to which trust companies are trustees: copy of trust deed and other prescribed information[66];
- for accounts of PEFPs: PEFP office or position and other prescribed information[67];
- for transactions of PEFPs: PEFP office or position and other prescribed information [68];
- for credit card accounts, account opening and accounts of PEFPs: PEFP office or position and other prescribed information [69];
- for foreign correspondent banking relationships: name and address and other prescribed information[70];
- for purchases from life insurance companies of immediate or deferred annuities or life insurance policies for which the client may pay $10,000 or more over the duration of the annuity or policy: client information record[71]; and
- for suspicious transactions and suspicious attempted transactions: investigations and conclusions.

FRFIs are expected to use record keeping methodologies and formats that are appropriate in their particular circumstances, provided that records required to be kept by the PCMLTFA and PCMLTFR must, as a general rule, be kept for at least 5 years[72] and they must be made available to competent authorities on a timely basis, which is within 30 days after a request is made[73].

[59] PCMLTFR p. 14(d
[60] PCMLTFR p. 14(e)-(h)
[61] PCMLTFR s. 14.1
[62] PCMLTFR p. 14(i)
[63] PCMLTFR p. 14(j)
[64] PCMLTFR p. 14(k) and (l)
[65] PCMLTFA p. 9.5(b)
[66] PCMLTFR ss. 15(1)
[67] PCMLTFR p. 14(n)
[68] PCMLFTR p. 14(o), s. 20.1
[69] PCMLTFR p. 14.1(g)
[70] PCMLTFR ss. 15.1(2)
[71] PCMLTFR s. 19
[72] PCMLTFR s. 69
[73] PCMLTFR s. 70

Client information should be kept current to reflect regulatory requirements and the FRFI's continuing knowledge of the client, client activities and purpose of the client relationship, which facilitates monitoring for suspicious transactions and attempted transactions.

A process should be implemented for dealing with incomplete documentation with a view to making it complete and current before doing more transactions or unrestricted transactions.

TRANSACTION REPORTING

General

The PCMLTFA and PCMLTFR prescribe reporting to FINTRAC on LCTRs, EFTs, STRs and TPRs.

FRFIs should ensure that internal reporting processes are designed to ensure compliance with regulatory reporting requirements as they relate to transaction reporting systems. Systemic compliance issues should be documented, escalated to the CAMLO and brought to the attention of FINTRAC. Control measures should include the identification of remedial action designed to eliminate compliance issues. For example, FRFIs should notify FINTRAC promptly of any internally identified LCTR, EFT or STR reporting errors or omissions. FRFIs should pay special attention to FINTRAC's error codes when filing reports, and take remedial action on a timely basis when FINTRAC indicates filing errors or other compliance issues. FRFIs should confirm to FINTRAC when remedial action is complete.

Suspicious Transactions and Suspicious Attempted Transactions, and Reports on Terrorist Property

Suspicious transactions and attempted transactions are defined in the PCMLTFA as those in respect of which there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of a ML offence or a TF offence.[74] There is no monetary threshold applicable to suspicious transactions or suspicious attempted transactions.

A transaction or attempted transaction that the FRFI reasonably suspects is related to a money laundering offence must be reported to FINTRAC. Property in the possession or control of a FRFI that the FRFIs knows, or has reasonable grounds to believe, is owned or controlled by or on behalf of a terrorist or a terrorist group, must also be reported to FINTRAC. This includes information about any transaction or proposed transaction relating to that property.

[74] PCMLTFA s. 7

The obligation to report suspicious transactions, suspicious attempted transactions and terrorist property[75]is designed to assist Canadian law enforcement authorities in their investigation and prosecution of ML and TF offences and predicate offences. Robust ongoing monitoring, examination and reporting processes in FRFIs are crucial in assisting these law enforcement efforts.

Suspicious transactions and suspicious attempted transactions should be identified by FRFIs from unusual activity or transactions. Procedures to identify unusual activities should capture the background and purpose of the transaction(s), who was involved, when and where it occurred, what products or services were involved and how the transaction was structured, and should be recorded.

STRs must be filed promptly in accordance with the regulatory requirements. Supporting documentation[76] must be retained as prescribed and made available to assist law enforcement authorities within prescribed deadlines.

FRFIs must ensure that information concerning STRs, including the fact that there is a suspicion and/or an STR, is kept strictly confidential. The client(s) involved must not be tipped off to a disclosure, and information within the FRFI must be strictly limited to the CAMLO and others on a "need to know" basis.

The PCMLTFR[77] require that, except where identity has been previously ascertained in accordance with the Regulations, FRFIs must take reasonable measures to ascertain the identity of every person with whom a suspicious transaction or suspicious attempted transaction is conducted. While reasonable measures may include normal client identification practices, care must be taken to ensure that such practices, if used, do not have the effect of tipping off the client.

Aggregation of Cash Transactions

The PCMLTFR provides[78] that where two or more cash transactions of less than $10,000 each are made within 24 consecutive hours that in the aggregate amount to $10,000 or more, the aggregated transactions are considered to be a single transaction of $10,000 or more for reporting purposes if a FRFI knows that the transactions are conducted by, or on behalf of, the same person or entity, or an employee or a senior officer of the FRFI knows that the transactions are conducted by, or on behalf of, the same person or entity.

For the purposes of interpreting this requirement, FRFIs that have systems in place that permit the FRFI to know, by making a record of multiple cash transactions referred to in this

[75] PCMLTFA s. 7 and s. 7.1
[76] Including a copy of the Suspicious Transaction Report
[77] PCMLTFR ss. 53.1(1)
[78] PCMLTFR ss. 3(1)

requirement, that the transactions are conducted by or on behalf of the same client should ensure that such transactions are aggregated and reported to FINTRAC as Large Cash Transactions.

TRAINING

Effective training programs for staff and others (as required) is an important and statutorily required element of FRFIs' AML/ATF programs.

FRFIs should ensure that written AML/ATF training programs are developed and maintained. Appropriate training should be considered for Senior Management, employees, agents and any other persons who may be responsible for control activity, outcomes or oversight, or who are authorized to act on the Company's behalf pursuant to the PCMLTFR[79]. The nature and content should be appropriate to the AML/ATF responsibilities of and the FRFI's relationship with, each intended recipient group. In particular, training should be tailored to provide the types and granularity of information and skills that are necessary for effective performance of the AML/ATF function in each case.

Training programs for Senior Management should provide sufficient briefing with respect to inherent risks and controls to enable them to assess information reported by the CAMLO and Auditor, and exercise effective oversight over the AML/ATF program.

SELF ASSESSMENT of CONTROLS

FRFIs should ensure that a self assessment of control measures is conducted, preferably on an ongoing basis, but at least annually. The assessment of AML/ATF controls is an important component of AML/ATF program because of its quality assurance outcome.

While the assessments in business areas can and should be conducted by individuals in those business areas, FRFIs should ensure that the assessment process is designed to enable results in each area to be consolidated for analysis and other purposes.

The self assessment in each relevant area of the FRFI should cover, at a minimum, the adequacy of the inherent risk assessment, AML/ATF policies and procedures, training and other controls implemented to mitigate ML and TF risks.

FRFIs should ensure that the self assessment is neither too narrow nor too broad. For example, a narrow legal/regulatory-based assessment could fail to cover broader ML and TF controls. Similarly an operational-based assessment might fail to cover prescribed controls.

All significant information used in the self assessment process should be verified or readily verifiable. Methods used to ensure that information is verified or verifiable will depend on the

[79] PCMLTFR p. 71(1)(d)

size, complexity and governance structure of the FRFI. Reasonably effective measures observed by OSFI tend to fall into one or more of the following categories:

1. Business areas are required by the CAMLO to provide information on the methodology they used to assess or re-assess ML and TF controls in their areas, in support of assessment results;
2. Business areas are required by the CAMLO to provide evidence of having documented support for the results of their assessments;
3. The CAMLO reviews and confirms the assessment results; or
4. A combination of the above.

The self assessment of controls should provide FRFIs with:

- Insight into the efficacy of controls in the AML/ATF program, and the overall extent to which the program adequately mitigates the identified inherent risks of ML and TF; and
- Information to aid in prioritizing remediation efforts if controls are under-performing and opportunities to capture economies of scale to better allocate resources to areas of higher risk.

EFFECTIVENESS TESTING

Like the assessments of inherent risk and risk management controls, effectiveness testing of the AML/ATF program is an important component of AML/ATF program quality assurance and is a statutorily required part of the FRFI's AML/ATF program.

The PCMLTFR[80] require that the following AML/ATF program components be reviewed for the purpose of testing their effectiveness every two years:

- Policies and Procedures;
- Risk assessments;
- Training programs.

The PCMLTFR[81] also prescribe minimum content and timing for reports to a senior officer on effectiveness testing.

In addition, it would be prudent for FRFIs to ensure that all other elements of the AML/ATF program be tested for effectiveness on a similar time scale.

FRFIs have access to internal or external auditors (or both) and therefore FRFIs should ensure that the Auditor is responsible for effectiveness testing. However, this does not preclude the Auditor from outsourcing all or part of the effectiveness testing to qualified third parties,

[80] PCMLTFR p. 71(1)(e)
[81] PCMLTFR ss. 71(2)

although remaining responsible for the effectiveness testing program. FRFIs should ensure that effectiveness testing of the AML/ATF program is included in the Auditor's mandate and audit program.

Effectiveness testing may be carried out on a stand-alone basis, or embedded in broader audits with other audit work. Whichever approach is taken, testing must cover all key AML/ATF program components, including policies and procedures, risk assessments and training programs at least every two years.

FRFIs should ensure that effectiveness testing is:

- in addition to (not a substitute for) assessments of inherent risks and risk management controls;
- appropriately risk based, with testing more frequently and/or thoroughly in higher risk categories throughout the FRFI as identified in the FRFI's Inherent Risk Assessment;
- planned and performed by an auditor or auditors who have had appropriate AML/ATF training and experience in respect of ML and TF risk and an appropriate level of knowledge of the regulatory requirements and guidelines; and
- reported to appropriate Senior Management, including information on testing scope, findings and recommendations or requirements for remedial action, and management's responses thereto.

Effectiveness Testing Compared To Assessment of Risks and Controls

The following table compares the different purposes, content, responsibility and outcomes of effectiveness testing and self-assessments of risks and controls:

	Effectiveness Testing	**Assessments of risks and Controls**
Purpose	Test the adequacy and effectiveness of AML/ATF program components in all relevant areas.	Assessing the scope and content of AML/ATF program components in all relevant areas.
By whom	Internal or External Auditor	Each relevant area And coordinated across the enterprise by the CAMLO
Frequency	Periodic; however at a minimum the FRFI must ensure the prescribed elements of the AML/ATF program are tested at least every two years.	Ongoing.
Reporting: timing and recipients	Within 30 days after work is complete, to Senior Management.	Within a reasonable time after work is complete, to Senior Management. At least once a year on a FRFI-wide basis by the CAMLO to Senior Management.

INTERPRETATION

The following meanings apply in this Guideline:

AML	Anti-money laundering
AML/ATF program	A FRFI's AML/ATF program designed to comply with this Guideline, and includes the program referred to in s. 71 of the PCMLTFR
ATF	Anti-terrorist financing
Auditor	The internal or external auditor of the FRFI responsible for effectiveness testing required by paragraph 71(1) (e) of the PCMLTFR
Board	Board of Directors. References to "Board" should be read as references to the Principal Officer of foreign bank branches and the Chief Agent of branches of foreign life insurance companies, as appropriate
CAMLO	The person designated responsible under PCMLTFR s. 71(1) (a) for implementing the FRFI's AML/ATF program, referred to by OSFI as the Chief Anti-Money Laundering Officer
CRA	Canada Revenue Agency
DTI	Deposit taking institution
EFT	Electronic funds transfer as defined in subsection 1(2) of the PCMLTFR
FATF	Financial Action Task Force on Money Laundering
FIU	Financial intelligence unit, and includes FINTRAC, as appropriate
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FRFI	Federally Regulated Financial Institution - includes banks, authorized foreign banks in respect of their business in Canada (foreign bank branches or FBBs), companies to which the *Trust and Loan Companies Act* applies, and life insurance companies or foreign life insurance company branches to which the *Insurance Companies Act* applies; and includes a FRFI's branches and subsidiaries world wide, if applicable.
LCM	Legislative compliance management
LCTR	Large cash transaction report
ML	Money laundering

OSFI Act	*Office of the Superintendent of Financial Institutions Act*
PCMLTFA	*Proceeds of Crime (Money Laundering) Terrorist Financing Act*
PCMLTFR	*Proceeds of Crime (Money Laundering) Terrorist Financing Regulations*
PEP	Politically Exposed Person
PEFP	Politically Exposed Foreign Person as defined in subsection 9.3(3) of the PCMLTFA.
STR	Suspicious transaction report and includes a report of a suspicious attempted transaction
Senior Management	Includes, but is not limited to, any person who is a senior officer as defined in the PCMLTFR
TF	Terrorist financing
TPR	Terrorist property report