Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

FINTRAC

Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing

March 19th, 2016

Canada

Table of Contents

Page

Introduction

The object of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its Regulations is to detect and deter money laundering and terrorism financing. In 2008, the Government of Canada introduced amendments to the PCMLTFA and its Regulations to enhance the Canadian anti-money laundering and anti-terrorism financing (AML/ATF) regime. As part of these amendments, the Risk-Based Approach (RBA), which requires reporting entities to conduct assessments of their exposure to money laundering and terrorism financing risk using a number of prescribed criteria, was introduced. These criteria are further discussed in this document. FINTRAC has also provided guidance on this matter in Guideline 4: *Implementation of a Compliance Regime*.

On the international front, the Financial Action Task Force (FATF), an inter-governmental body, has developed a series of *Recommendations* that are recognised as the international standard for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. More specifically, the FATF developed *Recommendation 1* on the RBA, an effective way to combat money laundering and terrorist financing.

By regularly assessing their money laundering and terrorism financing risks, reporting entities can protect and maintain the integrity of their businesses while contributing to the integrity of the Canadian financial system as a whole. While each reporting entity is responsible for its own risk assessment, FINTRAC has developed this guidance document to help reporting entities meet the RBA obligations.

This guidance document is structured to help reporting entities better understand what the RBA is and take inventory of their risks relating to products, services and delivery channels, clients and business relationships, geography and other relevant factors. It will also help in implementing effective mitigation measures and in monitoring the money laundering and terrorist financing risks reporting entities may have or encounter as part of their activities and business relationships.

This guidance document is intended for all activity sectors covered under the PCMLTFA. However, some examples and/or indicators may apply only to certain activity sectors.

Note: FINTRAC is developing sector-specific RBA workbooks that will help smaller reporting entities develop their RBA. These workbooks will be published on FINTRAC's website when available.

The Concept of Risk

What is risk?

Risk can be defined as the likelihood of an event and its consequences. In simple terms, risk can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result from such an occurrence. In the context of money laundering/terrorist financing (ML/TF), risk means:

- At the national level: threats and vulnerabilities presented by ML/TF that put at risk the integrity of Canada's financial system and the safety and security of Canadians.
- At the reporting entity level: threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF.

Threats: this could be a person (or group), object that could cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups.

Vulnerabilities: elements of a business that could be exploited by the identified threat. In the ML/TF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.

Impact: this refers to the seriousness of the damage that would occur if the ML/TF risk materializes (i.e. threats and vulnerabilities)

What is risk management?

Risk management is a process that is widely used in the public and private sector to assist in decision-making. When dealing with ML/TF, it is the process that includes the recognition of ML/TF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.

What are inherent and residual risks?

When assessing risk, it is important to distinguish between inherent risk and residual risk. Inherent risk is the intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures. On the other hand, residual risk is the level of risk that remains after the implementation of mitigation measures and controls. These concepts are further defined and explained in this guidance document. However, it is important to clarify that the risk assessment exercise described in this document focuses on the inherent risks to your business, activities and clients.

What is a risk-based approach?

In the context of ML/TF, a risk-based approach is a process that encompasses the following:

- The **risk assessment** of your business activities and clients using certain prescribed elements;
  - Products, services and delivery channels;
  - Geography;
  - Clients and business relationships[1]; and
  - Other relevant factors.
- The **mitigation of risk** through the implementation of controls and measures tailored to the identified risks;
- Keeping **client identification** and, if required, beneficial ownership and business relationship information up to date in accordance with the assessed level of risk; and
- The **ongoing monitoring** of transactions and business relationships in accordance with the assessed level of risk.

It is paramount to remember that assessing and mitigating the risk of ML and TF is not a static exercise. The risks that have been identified may change or evolve over time as new products or new threats enter your business context. Consequently, your risk-based approach should be re-evaluated and updated when the risk factors change.

[1] Business relationships are defined in section 6.3 of *Guideline 4: Implementation of a Compliance Regime*

General Overview and Purpose of this Guidance

By law, your compliance regime has to include:

1. the appointment of a compliance officer;
2. the development and application of compliance policies and procedures. These policies and procedures have to be written and kept up to date;
3. an assessment and the documentation of risks related to ML/TF, as well as the documentation and implementation of mitigation measures to deal with those risks;
4. an ongoing compliance training program (if you have employees or agents or other individuals authorized to act on your behalf). The training program has to be written and maintained; and
5. a review of your compliance policies and procedures to test their effectiveness. The review has to cover your policies and procedures, your assessment of risks related to money laundering and terrorist financing and your training program.

This guidance document will mainly focus on **item 3**: the assessment and documentation of risks related to ML/TF.

The nature of some of your business activities, and the business relationships you have with certain individuals exposes your business to ML and TF risks. In order to mitigate these risks, and to comply with the PCMLTFA and associated Regulations, your reporting entity must conduct a risk assessment. This will allow you to establish procedures and controls that will help detect and mitigate possible ML/TF activities.

It should be noted that conducting high-risk activities or having high-risk business relationships is not against the law. Defining clients as high-risk does not cast your business in a bad light; it is an assessment that allows you to ensure that controls are put in place to mitigate the risks and to apply prescribed special measures.

☑ This guidance document should help you:

1. Consider business-wide elements or factors that may impact your ML/TF risk and apply controls and measures to mitigate the risks, addressing:
    - **Your products, services and delivery channels**;
    - **Your business' geography**; and
    - **Other factors** relevant to your specific activities (e.g. legal, environmental, etc.)

2. Evaluate the risks associated with your **clients and business relationships** by looking at:
    - The products, services and delivery channels they utilize;
    - The geography related to your clients (their location, links to high-risk countries, where they conduct their business and transactions, etc.); and
    - Their activities, transaction patterns, characteristics, etc.

    This specific assessment will allow you to identify high-risk business relationships and apply the prescribed special measures.

3. Identify and validate controls to mitigate your high-risk activities and business relationships,

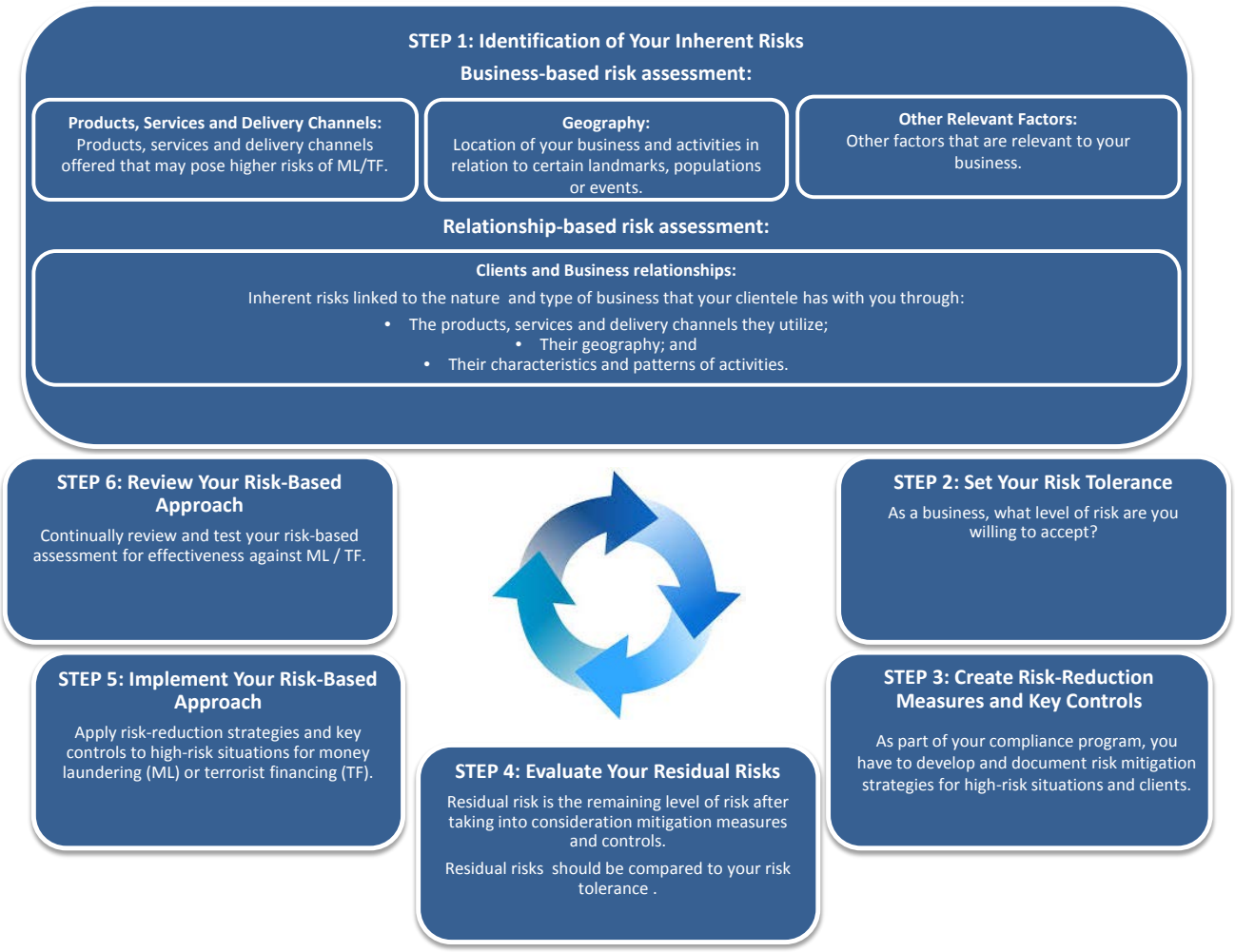
including prescribed special measures; and

4. Review and assess the status of your compliance regime with the PCMLTFA as well as the adequacy of your current controls to mitigate the identified high risks.

Risk-Based Approach Cycle

The following cycle represents the six steps of your risk-based approach:

1. identification of your inherent risks (business-based risk assessment along with the relationship-based risk assessment);
2. setting your risk tolerance;
3. creating risk-reduction measures and key controls;
4. evaluating your residual risks;
5. implementing your risk-based approach; and
6. reviewing your risk-based approach.



Overall FINTRAC expectations in regards to the RBA:

The expectations below are generic in nature. Please consult each specific step in this guidance document to better understand FINTRAC's expectations in each case.

- While there is no standard methodology, the outcome of your RBA should reflect the reality of your business, be documented and include all the prescribed elements (described on page 5). It is expected that in building a new or validating an existing RBA you will find this guidance useful to inform your risk assessment. However, entities should not find themselves limited to the information provided in this document in developing their own approach (provided that the information mandated by law or regulations is included); as long as the end-result of the risk assessment exercise is the same. FINTRAC expects a well-developed, documented and justifiable RBA process that appropriately identifies, rates and mitigates the risks to a given entity.

- Your RBA has to be tailored to your business size and type. For example, this means that FINTRAC would expect a more detailed methodology for reporting entities that conduct large volumes of transactions across various business lines and/or products.

- All steps and processes in relation to your RBA must be documented and decisions must be

supported by an appropriate rationale.

- You should establish sufficient capacity and expertise to support your risk-based approach. As risks will evolve over time, capacity and experience should also be expected to evolve.

- During an examination, FINTRAC may examine:
    - your risk assessment, your controls and mitigating measures including your policies and procedures, to assess the overall effectiveness of your risk assessment;
    - your business relationships and evaluate whether they have been properly assessed based on the products, services, delivery channels, geographical risk and other characteristics or patterns of activities;
    - your high-risk client files to ensure that the prescribed special measures have been followed and applied; and
    - sample records to assess whether monitoring and reporting are done in accordance with legislation, regulations and your policies and procedures.

Step 1: Identification of Inherent Risks

It is important to note that there is no prescribed methodology for the assessment of risks. What follows is FINTRAC's suggested model assessment process which will need to be adapted based on your business situation. Although presented separately, the steps below may be done simultaneously.

- **Business-based risk assessment**: your products, services and delivery channels, the geographical location in which your business operates along with other relevant factors.
- **Relationship-based risk assessment**: products and services your clients utilize, the geographical locations in which they operate or do business as well as their activities, transaction patterns, etc.

Business-based risk assessment

Identifying the inherent risks to your business will require you to look at your vulnerabilities to ML/TF.

Begin your risk assessment by taking a business-wide perspective. This will allow you to consider where risks occur across business lines, clientele or particular products. Areas identified as high-risk will require documented mitigation strategies.

Please note that the actual number of risks in your inventory will vary based on the type of business activity you conduct and products and services you offer.

The following pages highlight 3 elements of your risk assessment (products, services and delivery channels; geography; and other relevant factors) that should play a role in the analysis of your business risks.

☑ Ask yourself: What are the inherent risks of my business activities?

Please note the following lists are **not intended to be exhaustive** and should be adapted to take into account **all** of your products, services and delivery channels, geography and other relevant factors that may affect your business.

1- Products, Services and Delivery Channels:
You have to be aware of, and recognize products and services or combinations of them that may pose higher risks of ML/TF.

Examples	Points to consider
High-risk products and services, such as: • electronic funds transfers, • electronic cash, • letters of credit, • bank drafts, • front money accounts, • products offered through the use of intermediaries or agents,	Legitimate products and services can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. You may also want to assess the products and services by the type of market that they are directed to (e.g. corporations, individuals, business people, wholesale or

• private banking, • etc.	retail, etc.) as this may have an impact on the risk. Another question to ask yourself is whether the products or services allow your clients to conduct business or transactions with higher-risk business segments, or could they be used by your client on behalf of third parties? For more information, consult Guideline 4, Section 6 – Risk based approach.
Your business offers services such as international correspondent banking.	Foreign financial institutions are not always subject to the same regulatory framework as Canadian banks. As such, some of these foreign institutions may pose a higher money laundering risk to their respective Canadian financial institution correspondent(s). It is a known fact that foreign correspondent accounts have been used by criminals to launder proceeds of crime. In addition, shell companies can also be used in the layering process to hide the true ownership of the accounts at the foreign correspondent financial institutions, which can allow criminals and terrorists to more easily conceal the source and use of proceeds of crime. Without adequate controls, a Canadian financial institution may establish a traditional correspondent account with a foreign financial institution and not be aware that the foreign financial institution is allowing customers to conduct anonymous transactions through the Canadian bank account. It is paramount for Canadian financial institutions offering foreign correspondent banking services to have policies, procedures, and processes to manage the inherent risk of these relationships. For more information, please consult section 9 of Guideline 6G: http://www.fintrac-canafe.gc.ca/publications/guide/Guide6/6G-eng.asp
Delivery channels, such as: • Non face-to-face transactions • Agent network	You may have a higher inherent risk in regards to your delivery channels if you offer non face-to-face transactions, use agents or if clients can apply for products online. This is especially true if you rely on an agent (that may or may not be covered by the PCMLTFA) to identify your clients. For the purpose of the PCMLTFA, a reporting entity is

	accountable for the activities conducted by its agents. In addition, new delivery channels (e.g. for products or services such as virtual currency) may have inherently higher risks for ML/TF due to the anonymous nature of non-face to face transactions.
New Technologies	Your business may be offering products/services that are based on new technologies that may have an impact on your overall inherent risks. For example, new payment methods can be used to transmit funds more quickly or anonymously, such as electronic wallets, pre-paid cards, internet payment services, digital currency or mobile payments.

2- Geography:
Location of your business relative to certain landmarks, populations or events

Examples	**Points to consider**
Border-crossings: • Air (i.e. airports) • Water (i.e. ports, marinas) • Land (i.e. land border-crossings) • Rail (i.e. passenger and cargo)	If your business is situated near a border-crossing, you may have a higher inherent risk due to the fact that your business may be the first point of entry into the Canadian financial system. This does not mean that you should assess all activities and all clients as high-risk due to the fact that your business is located near a border crossing or major airport. FINTRAC is simply highlighting the fact that such businesses may want to pay closer attention to the fact that their geographical location may impact their business (as an example, this could be done through training so that staff better understand the placement stage of money laundering and potential impacts).
Geographical location and demographics: • Large city • Rural area	Your geographical location may also impact your overall business risks. Depending on your situation, a rural area where clients are known to you could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime would obviously have the reverse effect. Some provincial governments have interactive maps detailing crime by regions which may inform and benefit your assessment.

	Example for Québec: http://geoegl.msp.gouv.qc.ca/dpop/ Other websites (such as Statistics Canada) provide good information on crime in Canada and also provide statistics and trends by province. Crimes, by type of violation, and by province and territory: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/legal50b-eng.htm Police-reported crime statistics in Canada, 2013: http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14040-eng.htm
Your business is located in an area known for its high crime rate	High crime areas need to be reflected in the overall assessment of your business as they may present additional ML/TF risks. The following websites (sample only) provide an overview of what can be found online in relation to crime in city areas or neighborhoods. Please note that statistics like the ones below are not necessarily offences linked to ML/TF but rather provide a general view of where crime occurs within a city. Vancouver: http://vancouver.ca/police/organization/planning-research-audit/neighbourhood-statistics.html Edmonton: http://crimemapping.edmontonpolice.ca/ Calgary: http://www.calgary.ca/cps/Pages/Statistics/Calgary-Police-statistical-reports.aspx# Winnipeg: http://www.winnipeg.ca/crimestat/ Toronto: http://www.torontopolice.on.ca/statistics/stats.php Ottawa: http://www.ottawapolice.ca/en/crime/crime-stats.asp Montreal: http://www.spvm.qc.ca/RapportAnnuel/2013/ Halifax:

	http://maps.halifax.ca/crimemapping/ Not every client from a higher crime area must be considered high-risk. Reporting entities simply need to be aware of their surroundings and how these could impact their activities. An online search on crime related statistics in your city or area should provide you with links to sources that you can consult in this regard (for example, municipal police departments or other databases).
Events and patterns	Depending on the population and demographics of your business, are there events or patterns (either domestic or international) that could impact your business? Example: you may be dealing with clients that have a relation to high-risk jurisdictions or other jurisdictions that are currently dealing with specific events (e.g. prevalence of terrorism or money laundering, war, etc.). Not all activities and clients need be classified as high-risk in relation to an event, conflict or high-risk jurisdiction. Businesses may want to be aware of these activities or transactions for anything unusual.
Connection to high-risk countries: • UN Security Council Resolutions • Special Economic Measures Act (SEMA) • Financial Action Task Force (FATF) list of High-Risk Countries and Non-Cooperative Jurisdictions • Freezing Assets of Corrupt Foreign Officials Act Sanctions (FACFOA)	International fora may impact future mitigation measures aimed at the detection and deterrence of ML/TF. Certain countries should be identified as posing a high risk for ML/TF based on, among other things, their level of corruption, the prevalence of crime in their region, the weaknesses of their money laundering control regime, or being identified by competent authorities like the FATF or FINTRAC through their respective advisories. However, if you or your clients have no connections to these countries, the risk is likely to be low or non-existent for that specific element. Canadian Economic Sanctions: http://www.international.gc.ca/sanctions/index.aspx High-Risk and Non-Cooperative Jurisdictions: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/ FINTRAC Advisories: http://www.fintrac-canafe.gc.ca/new-neuf/avs/1-eng.asp Security Council Resolutions:

http://www.un.org/en/sc/documents/resolutions/index.shtml

Freezing Assets of Corrupt Foreign Officials Act Sanctions: http://www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/snc/facfo-bbde/Pages/default.aspx

3- Other Relevant Factors (if applicable):

Other factors that could be relevant to your business and have an impact on the risk of ML/TF, such as:

- **legal**: related to domestic laws, regulations, and potential threats
- **structural**: related to specific business models and processes

Examples	Points to consider
• Special Economic Measures Act (SEMA) • Ministerial Directives • Regulators • National Risk Assessment	Sanctions can impact your business by: • prohibiting trade and other economic activity with a foreign market, • restricting financial transactions such as foreign investments or acquisitions, or • leading to the seizure of property situated in Canada. These restrictions may apply to dealings with entire countries, non-state actors, such as terrorist organizations, or designated persons from a target country. As part of your risk assessment, you must take into consideration any ministerial directives. If your business is prudentially regulated, you may have additional measures to follow as specified by your sector Regulator. Example: the Office of the Superintendent of the Financial Institutions of Canada (OSFI) has published Guideline B-8 for financial institutions. Assessment of Inherent Risks of ML/TF in Canada: The national risk assessment informs and assesses the ML/TF risks in Canada which may help you identify potential links to your own business activities.
Trends, typologies and potential threats of ML/TF: • ML/TF methods used in specific sectors	Trends and typologies for your respective activity sector may include specific elements of risks that

- Main ML/TF actors including organized crime groups, terrorist organizations, facilitators, etc.
- Corruption and other crimes

your business should consider.

FINTRAC Typologies and Trends Reports (not available for all activity sectors): http://www.fintrac-canafe.gc.ca/publications/typologies/1-eng.asp

FATF Methods and Trends (not available for all activity sectors): http://www.fatf-gafi.org/topics/methodsandtrends/

Not all elements listed in these trends and typologies will affect you but you should be aware of the high-risk indicators that may have an impact on your business.

Business model:

- Operational structure
- Third party and/or service providers

You will need to consider your business model, the size of your business, the number of branches and employees, to determine if risks exist in relation to this element.

Examples:

- A business with hundreds of branches and thousands of employees will present different risks than a business that has one location and 2 employees.
- A business with a high employee turnover.

These examples highlight the fact that other compliance regime elements such as training are very much intertwined with your RBA exercise. Since training should give employees an understanding of the reporting, client identification, record keeping requirements, and an understanding of the penalties for not meeting those requirements, having numerous branches and/or a high employee turnover is a risk that should be tackled in your training program.

It is also important to remember that although the use of a third party or service provider can be a good business practice, your business is ultimately responsible for the compliance regime, client identification, record keeping and reporting obligations. You will want to ensure that you fully understand how your third party/service provider is functioning.

Scoring your business-based risk assessment

Once you have identified and documented all the inherent risks as explained in the business-based risk assessment described previously, you will need to attribute a level to each risk. A risk scale must be established, tailored to the size and type of business you have. Very small businesses engaged in occasional straightforward transactions may only require distinguishing between low and high risk categories. Larger businesses are expected to establish more risk categories if warranted (e.g. medium, medium-high, high, etc.).

☑ By law, every risk element identified as "high-risk" must be addressed with mitigation measures and be documented.

☑ You will have to be able to demonstrate to FINTRAC that controls/measures have been put in place to address these high-risk elements (e.g. in your policies and procedures, training program) and that they are effective (through your internal or independent review).

References:

1-The table in Annex B lists **some** risk factors that you could encounter as a business and provides a rationale as to how you could differentiate between low, medium or high risk categories.

2-To help you with the evaluation of your business risk assessment, you can use a likelihood and impact matrix tool similar to the one presented in Annex C.

Relationships-based risk assessment

Once your business-based risk assessment is completed you can focus on the last element of your risk assessment: your clients. When you enter into a business relationship with a client, you have to keep a record of the purpose and intended nature of the business relationship. You also have to review this information on a periodic basis. This will help you determine the risk of ML/TF, as well as understand the patterns and transaction activities of your clients. Although documenting the business relationship is a record keeping requirement, it will ultimately help REs in the monitoring stage where activities/transactions can be compared to the purpose and intended use of an account, occupation, etc.

The overall relationship-based risk assessment includes the following:

1. The risk posed by the combination of products, services and delivery channels the client uses;
2. The risk posed by the geographical location of the client and of his or her transactions; and
3. The risk posed by the client's characteristics, patterns of transactions, etc.

☑ The relationship-based risk assessment ultimately combines products, services, delivery channels, and the client's geographical risk. This should help you in determining the risk score of your clients or business relationship.

☑ For more information on business relationships, please consult sections 6.3 and 6.4 of *Guideline 4: Implementation of a Compliance Regime* and *Guideline 6: Record Keeping and Client Identification*.

1. Products, Services and Delivery Channels:

In the business-based risk assessment, you have identified high-risk products, services, and delivery channels. You will need to mitigate the risk they pose. In the relationship-based risk assessment, we are looking at the

products, services and delivery channels that your clients or business relationships are using and their impact on their overall risk.

Product Risks:

Products will have a high inherent risk where there is client anonymity or when the source of funds is unknown.

Where possible, it is advisable that a review of the products be completed with the employees who handle them to ensure the completeness of the risk assessment.

Service Risks:

Where governmental authorities or other credible sources have identified a service as being potentially high-risk for ML/TF, this should be taken into account during the risk assessment.

For example, high-risk services include: electronic funds transfers, international correspondent banking services, international private banking services, services involving banknote and precious metal trading and delivery, front money accounts for casinos, etc.

Delivery Channel Risks:

A delivery channel is a medium that can be used to obtain a product or service, or through which transactions can be conducted. Delivery channels should be considered as part of the risk of the transactions. Delivery channels allowing for non-face-to-face transactions have a higher inherent risk.

Many delivery channels do not bring the client into direct face-to-face contact with you (for example, internet, telephone or new products such as virtual currency), and are accessible 24 hours a day, 7 days a week, from almost anywhere. This can be used to obscure the true identity of a client or beneficial owner and can therefore pose higher risks. Although some delivery channels may have become the norm (e.g. use of internet for banking), it should nonetheless be considered as part of a combination of factors that could make a specific element or client high-risk.

☑ Below are some products, services and delivery channels that inherently pose a higher risk. Please note that the following list is **not intended to be exhaustive** and should be adapted to take into account all of your organization's products, services and delivery channels.

To help you with the overall risk assessment of a client or group of clients, you should also consider known risk factors that can **increase** the overall risks of ML/TF such as:

- Criminal antecedents of the client in regards to a designated offence [2]
- Unknown source of funds
- The anonymity of a beneficiary
- The anonymity of the individual conducting the transaction

[2] See Guideline 1 – Section 2.1 for more details

- The absence of detail in the transaction records
- Unusual speed, volume and frequency of transactions
- Unexplained complexity of accounts of transactions

Similarly, you should also look at factors that can **decrease** the risks of ML/TF, such as:

- A low volume of activity
- A low aggregate balance
- Household expense accounts or accounts for the investments of funds that are subject to a regulatory scheme (for ex., Registered Retirement Savings Plan)

High-Risk Indicators	**Rationale**[3]
Your clients utilize electronic funds payment services such as: • electronic funds transfers • electronic cash (e.g. stored value cards and payroll cards)	**Electronic funds transfers** can be done in a non-face-to-face environment. Additionally, large amounts of money can be transmitted outside of Canada or into Canada, which can disguise the origin of the funds. **Electronic cash** is a high-risk service because it can allow parties to conduct transactions without being identified.
Your clients utilize products such as bank drafts and letters of credit.	**Bank drafts** can move large amounts of funds in bearer form without the bulkiness of cash. These products are much like cash in the sense that the holder of the draft is the owner of the money. For example, an individual obtains a 100,000 dollar bank draft (showing a financial institution as the payee) and passes it on to another person. This process could effectively blur the trail of money. However, if the bank drafts issued are payable to specific payees only, the inherent risk of this product is mitigated. **Letters of credit** are essentially a guarantee from a bank that a seller will receive payment for goods. Although guaranteed by a bank, letters of credit have a higher inherent risk for ML/TF as they can be used in trade-based transactions to increase the appearance of legitimacy and reduce the risk of detection. Money Launderers using a trade-based transaction (e.g. seller/importer) may also include under/over valuation schemes which will allow them to move their money under this veil of legitimacy. There is also heightened risk when the use of a letter of credit is not consistent with the usual pattern of activity of the client.
Your clients use some products and services that you offer through non-face to face channels or through the	Non-face to face transactions make it more difficult to ascertain the identity of your clients.

[3] Rationale could also include reference to a website, a publication, a report, etc.

use of intermediaries, agents or introducers.	In addition, the use of intermediaries or agents may increase your inherent risks as they may not be subject to anti-money laundering and anti-terrorist financing (AML/ATF) laws and measures and may not be adequately supervised. It is important to note that for the purpose of the PCMLTFA, a reporting entity is accountable for the activities conducted by all of its agents. As a result, reporting entities will want to ensure that their agents meet their compliance obligations on an ongoing basis. Furthermore, the reporting entity should have proper due diligence (e.g. background checks and ongoing monitoring) in place to lessen the risk of being used for ML/TF purposes through its agent network.
Your clients utilize front money accounts (Casino sector).	Front money accounts allow customers to deposit money at a casino. Customers can draw upon the accounts for gaming purposes. This service is convenient and increases security, as customers do not have to travel to and from the casino carrying large amounts of cash. Money launderers and other criminals may believe that, despite similarities to accounts held at financial institutions, front money accounts are subject to less scrutiny than accounts at financial institutions used for the same purposes. Examples: • A customer deposits cash, a cheque or bank draft made payable to the casino or to himself, to a front money account, and later withdraws all or part of the funds, with minimal or no gaming observed. • A customer deposits small denomination bills to a front money account, and later withdraws the funds in higher denomination bills; • A third party makes frequent cash deposits (below the reporting threshold) to a customer's front money account.

2. Geography

In the business-based risk assessment, you have identified high-risk elements relating to the geographical location of your business. In the relationship-based risk assessment, we are looking at the geography of your clients or business relationships and its impact on their overall risk.

Your business faces increased ML/TF risks when funds are received from or destined to high-risk jurisdictions, and when a client has a material connection to a high-risk country. As such, risks associated with residency, citizenship or transactions should be assessed as part of the inherent risk of your clients.

☑ The following are some elements that you should consider (please note the following list is **not intended to be exhaustive** and should be adapted to take into account all aspects of your clients' geography):

High-Risk Indicators	Rationale
Your client's proximity to a branch.	A client that conducts business or transactions away from their home branch without reasonable explanation should be noticed. For example, one of your clients, a small single location business makes deposits on the same day at different branches across a broad geographical area that does not appear practical.
Your client is a non-resident.	Identification of these clients may prove more difficult since they may not be present and as such, should raise the inherent level of risk.
Your client has offshore business activities or interests.	Is there a legitimate reason for this? Offshore activities may be used by a person to add a layer of complexity to transactions, thus raising the overall risk of ML/TF.
Your client's connection to high-risk countries.	Your client's connection to high-risk countries should be taken into account as some countries have weaker or inadequate anti-money laundering and anti-terrorist financing standards, insufficient regulatory supervision, or simply present a greater risk for crime, corruption or terrorist financing.

3. Clients Characteristics and Patterns of Activity:

At the beginning of a client relationship, and periodically throughout the relationship (your policies and procedures must reflect this), you should consider the purpose and intended nature of your business relationships (i.e. understand your clients' activities and transaction patterns) in order to determine their level of ML/TF risk.

Some characteristics or patterns of activities will have an inherently higher risk of ML/TF and must be considered when assessing the overall risk of a client or business relationship.

☑ **IMPORTANT:** Below are three indicators that will automatically place clients in the high-risk category:

High-Risk Indicators	Rationale
Your client is in possession or control of property that you **know / believe** is owned or controlled by or on behalf of a terrorist or a terrorist group	You are required to send a terrorist property report to FINTRAC if you have property in your possession or control that you **know / believe** is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about transactions or proposed transactions relating to that property. Once a TPR is filed, the client automatically becomes high-risk.
Your client is a Politically Exposed Foreign Person (PEFP)	A PEFP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence that they may hold, a PEFP is vulnerable to ML/TF or other offences such as corruption. As a business, you must consider a politically exposed

	foreign person as a high-risk client.
The entity has a complex structure that conceals the identity of beneficial owners	Modifications have been made to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* (PCMLTFR), effective February 2014, in regards to ownership and control of a corporation or an entity. When the information cannot be obtained or cannot be confirmed, your business will be required to "ascertain the identity of the most senior managing officer of the entity" and treat the entity as high-risk, and apply the newly prescribed special measures as stated in the PCMLTFR. For more information, please consult section 6.3 of Guideline 4: http://www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp#s663 ☑ This indicator applies only to financial entities, securities dealers, the life insurance sector, and money service businesses. It is important to note that although you may have the information on beneficial ownership, you may have additional information or indicators that would make this relationship a high-risk one.

☑ The following table contains additional indicators of high risk (please note the following list is **not intended to be exhaustive** and should be adapted to your organization):

High-Risk Indicators	**Rationale**
A suspicious Transaction Report (STR) was previously filed or considered	Suspicious transactions (or attempted transactions) are financial transactions that you have reasonable grounds to suspect are related to the commission of a **money laundering or terrorist activity financing offence**. STRs on file should elevate the risk of the client or business relationship.
Transactions involving third parties	There can be suspicion when it comes to transactions involving third parties. For securities dealers (as an example), suspicion in relation to third parties may relate to the source of funds deposited to securities accounts, or to the use of funds following withdrawals from securities accounts. Example: • incoming electronic funds transfers (EFTs) from, or outgoing EFTs to, third parties; • transfers to/from securities accounts held by third parties; and • negotiable instruments (e.g. certified cheques, bank drafts) made payable to third parties. Transactions of this nature within your activity sector could be

	indicative of the layering stage of money laundering activity.
The account activity does not match the client profile	Account activity that doesn't match the client profile may indicate a higher risk of ML/TF. Your entity may be faced with situations where it has made several Large Cash Transaction Reports (LCTRs) about a client with an occupation that does not match this type of activity (e.g. student, unemployed, etc.)
Your client's business generates cash for transactions not normally cash intensive	The fact that there is no legitimate reason for the business to generate cash represents a higher risk of ML/TF.
Your client's business is a cash-intensive business (e.g. bars, clubs, etc.)	Certain types of business, especially those that are cash-intensive may have a higher inherent risk for ML/TF. Example: Clients that own white label ATMs.
Your client offers online gambling	Industry intelligence, including reports from the Royal Canadian Mounted Police, indicates that, due to the nature of the business, the gambling sector is susceptible to money laundering activity. Additionally, FATF has indicated that 'internet payment systems' are an emerging risk in the gambling industry. Internet payment systems are used to conduct transactions related to online gambling, these two factors making the online gambling industry inherently high-risk. Higher inherent risk may exist if the online gambling activities are not managed by provincial lottery and gaming corporations.
Your client's business structure (or even transactions) seems unusually or unnecessarily complex	An unnecessarily complex structure or the complexity of a client's transactions (compared to what you normally see in a similar circumstance) may indicate that the client is trying to hide transactions and/or suspicious activities. Example for a securities dealer: • frequent contributions and withdrawals from securities accounts, • transfers between accounts for no particular reason.
Your client is a financial institution with which you have a correspondent banking relationship and/or	Some countries have weaker or inadequate anti-money laundering and anti-terrorist financing standards, insufficient regulatory supervision, or simply present a greater risk for crime, corruption or terrorist financing. Additionally, the nature of the businesses that your correspondent bank client engages in, as well as the type of markets it serves, may present greater risks.

Your client is a correspondent bank that has been subject to sanctions	The fact that your client has been subject to sanctions should raise the risk level and appropriate measures should be put in place to monitor the account.
Your client is a reporting entity under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) that is not otherwise regulated	Some reporting entities that are not federally or provincially regulated (other than under the PCMLTFA) may present higher risks of ML/TF. In addition, some may have cash intensive businesses that may also increase the overall risks of ML/TF.
Your client is an intermediary or a gatekeeper (ex. lawyer or accountant) holding accounts for others unknown to you	Accountants, lawyers and other professionals sometimes hold co-mingled funds accounts where the beneficial ownership may be difficult to verify. This doesn't mean that all clients with these occupations are high-risk. Understanding that risk exists for these occupations, it will be up to you to determine if the activities and/or characteristics of these clients are in line with what you would expect.
Your client is an unregistered charity	Charities can be misused by individuals or other organizations to assist in money laundering schemes or finance/support terrorist activity. It is important to be aware of the risks in relation to charities, and to apply due diligence by confirming that the charity is registered with the Canada Revenue Agency.

Scoring your relationship-based risk assessment

Under the relationship-based assessment, **every** high-risk client (or group of clients) will need prescribed special measures (see step 3). These measures will have to be documented in your policies and procedures and applied to your high-risk clients/relationships.

You can assess the ML/TF risk for each individual client or for groups of clients. Where possible, this assessment could take the form of establishing clusters (or groups) of clients having similar characteristics using different risk variables. For example, clients with similar income and portfolios of accounts or conducting similar types of transactions could be grouped together. This approach can be especially practical for financial institutions.

☑ It is important to remember that identifying one high-risk indicator for a client doesn't necessarily mean that you now have a high-risk client relationship (except for the elements outlined on pages 20-21). Your relationship-based risk assessment model ultimately **draws together** the products, services and delivery channels used by your client; your client's geographical risk; and your client's characteristics and patterns of activities. It is up to you to determine how to best assess the risk of each client or groups of clients.

Reference:

1-To help you with the assessment of your relationship-based risk assessment, you can use a likelihood and impact matrix tool similar to the one presented in Annex C.

FINTRAC expectations for Step 1 – Identification of your inherent risks:

As part of Step 1, FINTRAC expectations are that:

- You have considered and assessed your business risks (products, services and delivery channels; geography, and other factors relevant to your business) and are able to explain and provide a rationale. Every high-risk element identified will need to be mitigated by controls or measures and be documented.
- You have considered and assessed your clients or business relationships based on the products, services and delivery channels used by your client; geographical elements related to your client; and your client's characteristics and patterns of activities.
    - You can demonstrate that you have assessed the risks of each individual client or group of clients with which you have a business relationship.
    - Assessing groups of clients or business relationships that share similar characteristics is fine as long as you can demonstrate that the groupings are logical and specific enough to **reflect the reality of your business**.
- You can provide documented information that demonstrates that you have considered high-risk indicators (such as the ones contained in this guidance document where applicable) in your assessment.
- In situations where high-risk indicators are not considered (i.e. FINTRAC considers a specific element as high-risk but you decide to downgrade the same element), you must be able to provide reasonable rationale for your decision.
- For every high-risk relationship, prescribed special measures must be put in place and documented as part of your policies and procedures.
- The use of a checklist is acceptable as long as you are able to provide a documented analysis of the risk and draw conclusions as to ML/TF threats and vulnerabilities to which your business is exposed, based on products, services, delivery channels, geographical locations, relationships-based risks (i.e. your clients) and other relevant factors.
- If your business is using a service provider to perform a risk assessment of your business and clients on your behalf, you need to understand that there may be vulnerabilities associated with this as your business is ultimately responsible for the risk assessment obligation.

Step 2: Set your Risk Tolerance

Risk tolerance is an important component of effective risk management. It is paramount to take your risk tolerance into account before moving on to considering how risks can be addressed. When considering threats, the concept of risk tolerance will allow you to determine the level of exposure (e.g. number of high-risk clients, inherently high-risk products, etc.) that you consider tolerable.

To do so, you may want to consider the following risk categories that could affect your organization:

- Regulatory risk
- Reputational risk
- Legal risk
- Financial risk

It is important to note that the PCMLTFA and Regulations state that your organization has mandatory obligations in situations where high-risk business activities and high-risk business relationships are identified. This step does not allow reporting entities to avoid these obligations.

Similarly, there is nothing in the PCMLTFA and Regulations preventing you from having a high-risk tolerance. If your business is willing to deal with high-risk situations and/or clients, FINTRAC will simply expect that the mitigation measures or controls put in place (see step 3) will be commensurate to the high risks that your entity is dealing with.

☑ Some of the questions that you may want to answer are:

- Is your entity willing to accept regulatory, reputational, legal or financial risks?
- What risks is your entity willing to accept only after implementing some mitigation measures?
- What risks is your entity not willing to accept?

This should help you determine your overall risk tolerance (notwithstanding your mandatory obligations).

FINTRAC expectations for Step 2 – Set your risk tolerance:

As part of Step 2, FINTRAC expectations are that:

- As a best practice, FINTRAC strongly suggests that entities take the time to establish their risk tolerance as it is an important component for achieving effective risk management (establishing a risk tolerance is not a legislative requirement).

- Your risk tolerance will have a direct impact on the following step: creating risk-reduction measures and key controls, your policies and procedures, and training.

- Determining your risk tolerance is an exercise that should include obtaining senior management approval.

Step 3: Create Risk-Reduction Measures and Key Controls

Risk mitigation is about implementing controls to limit the ML/TF risks you have identified while conducting your risk assessment. The risk mitigation will also allow your business to stay within the risk tolerance you have identified. When your risk assessment determines that risk is high for ML/TF, you will have to develop written risk mitigation strategies (policies and procedures designed to mitigate high risks) and apply them to the high-risk situations or business relationships you have identified.

It is important to note that having a high-risk tolerance (step 2) and being willing to deal with high-risk situations and/or clients should lead to stronger mitigation measures and controls. The overall expectation is that the mitigation measures and controls will be commensurate with the risks that have been identified.

1. **In all situations,** your business should consider internal controls that will help in mitigating your overall risk. Examples of such controls are included in section 6.2 of Guideline 4.

2. **For your business-based risk assessment,** all high-risk elements that you have identified as part of your assessment will have to be mitigated by controls or measures and be documented.

3. **For all your clients and business relationships**, you will be required to:
    a. Conduct ongoing monitoring for all your business relationships.
    b. Keep a record of the measures and information obtained.

4. **For your high-risk clients and business relationships)**, you will be required to adopt the following prescribed special measures:
    a. Conduct **more frequent** monitoring of your business relationship.
    b. Take enhanced measures to ascertain the identification and/or keep client information up to date (examples of measures can be found subsection 6.4 of Guideline 4)

☑ For **detailed** information on risk mitigation measures, please consult sections 6.2, 6.3 and 6.4 of *Guideline 4: Implementation of a Compliance Regime*.

FINTRAC expectations for Step 3 – Create risk-reduction measures and key controls:

As part of Step 3, FINTRAC expectations are that you:

- Keep client identification and beneficial ownership information up to date.
- Establish and conduct the appropriate level of ongoing monitoring for your business relationships (on a periodic basis for lower risk clients and more frequent for high-risk clients).
- Implement mitigation measures for situations where the risk of ML/TF is high (business-based or client relationships). These written mitigation strategies must be included and documented in your policies and procedures.
- Apply these controls and procedures consistently as FINTRAC may assess them via transaction testing.

Step 4: Evaluate Your Residual Risks

Residual risk is the risk remaining after taking into consideration risk mitigation measures and controls. It is important to note that no matter how robust your risk mitigation and risk management program is, your business will always have some exposure to residual ML/TF risk which you must manage.

Residual risks should be in line with your overall risk tolerance as explained in step 2. You will want to ensure that the risks you are left with are not greater than what you are prepared to tolerate to do business. If you realize that the level of residual risk is still greater than your overall tolerance; or that your measures and controls do not mitigate the high-risk situations or clients sufficiently, you must go back to step 3 and increase the level and/or quantity of mitigation measures that were put in place.

As stated, if your business is willing to deal with high-risk situations and/or clients, FINTRAC will simply expect that the mitigation measures or controls put in place (see step 3) be commensurate, and that the residual risks are reasonable and acceptable.

☑ Types of residual risk:

- **Tolerated** risks: Although they are "tolerated", they are still risks. Acceptance means there is no benefit in trying to reduce them. However, the tolerated risks may increase over time, for example, when a new product is introduced or a new threat appears.

- **Mitigated** risks: Although they are "mitigated", they are still risks. These risks have been reduced but not eliminated. In practice, the controls put in place may fail from time to time (for example, your monitoring system or transaction review process fails and some transactions are not reported).

Example:

Business A offers electronic funds transfers as a service to its clients. Reporting systems are in place to capture transactions of $10,000 or more, and policies and procedures have been developed to properly ascertain the identity of individuals when they conduct a remittance or transmission of $1,000 or more. The reporting system is also in place to identify transactions that could be suspected to be related to a money laundering or terrorist financing offence (for suspicious transaction reporting purposes).

Since Business A considers electronic funds transfers to be a high risk service, it added a mitigation measure to control the risk associated with the service. The staff (through the training program) is reminded regularly of the risks associated with international electronic funds transfers and are made aware of updates/changes to high-risk jurisdictions as indicated in the various advisories released by the government. These measures were put in place a few years ago and are well understood and followed by the staff.

In this example, the mitigation measures put in place were, at the time, in line with the risk tolerance of Business A in regards to electronic funds transfers. As such, the residual risk was tolerable for Business A.

However, as risk or clientele evolves over time, Business A now feels that the mitigation measures are no longer sufficient to meet their risk tolerance. In fact, Business A's risk tolerance is now lower than it used to be (i.e. they are less inclined to take on high-risk elements). This means that the residual risks from the previously established mitigation measures now exceed the new risk tolerance.

Business A will add new mitigation measures to realign the residual risk with its new tolerance level. Some examples of measures are:

- Put a limit on specific transactions (e.g. electronic funds transfers to specific jurisdictions)

- Require additional internal approvals for certain transactions; and/or
- Monitor some transactions more frequently to help reduce the risk of structuring (e.g. a $12,000 transaction that is split into two $6,000 transactions to avoid reporting).

FINTRAC expectations for Step 4 – Evaluate your residual risks:

As part of Step 4, FINTRAC expectations are that:

- As a best practice, FINTRAC strongly suggests that reporting entities take the time to evaluate their level of residual risks (evaluating your residual risk is not a legislative requirement).

- Reporting entities should confirm that the level of risk is aligned with what they are willing to tolerate (as described in step 2) to ensure the integrity of their own business.

Step 5: Implement Your Risk-Based Approach

Once you have gone through the risk assessment exercise, you will implement your risk-based approach as part of your day-to-day activities. In addition to your newly implemented risk-based approach, existing obligations, such as client identification, need to be maintained as a minimum baseline requirement.

To be effective, your risk assessment must be documented as part of your compliance regime. A detailed and well documented compliance regime shows your commitment to prevent, detect and address non-compliance within your organization.

It is important that your compliance policies and procedures are communicated, understood and adhered to by all the staff dealing with clients. This includes those who work in the areas relating to client identification, record keeping, and the types of transactions that have to be reported to FINTRAC. They need enough information to process and complete a transaction properly, as well as to identify clients and keep records as required.

Your compliance policies and procedures should incorporate, at a minimum, the requirements for:

- reporting,
- recordkeeping,
- client identification,
- risk assessment and
- special measures for high risks.

Your policies and procedures should also:

- Explain how to detect suspicious transactions and your process for dealing with such situations;
- Determine and explain what kind of monitoring is done for particular situations (i.e. low vs. high-risk clients / business relationships);
- Describe all aspects of your monitoring:
    - when it is done (its frequency),
    - how it is conducted, and
    - how it is reviewed.

As a reminder, this means that you will have to conduct ongoing monitoring of all your business relationships and enhanced ongoing monitoring for the business relationships that pose high risks of ML/TF. You will also have to apply prescribed special measures for your high-risk clients/relationships.

It is also important to remember that the approach to the management of risk and risk mitigation requires the leadership and engagement of senior management. Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of ML/TF within a business.

☑ For more information, please consult *Guideline 4: Implementation of a Compliance Regime*.

FINTRAC expectations for Step 5 – Implement your risk-based approach:

As part of Step 5, FINTRAC expectations are that you:

- Ensure that your risk assessment describes your RBA process, the frequency of your monitoring for low and high-risk clients, as well as describes the measures and controls put in place to mitigate the high risks that have been identified as part of step 1.
- Apply your RBA as described in your documentation.
- Keep client identification and beneficial ownership documentation up to date.
- Conduct ongoing monitoring of all your business relationships.
- Conduct more frequent ongoing monitoring of your business relationships that pose a high-risk of money laundering and terrorist financing.
- Apply appropriate prescribed special measures for your high-risk clients.
- Involve senior management when dealing with high-risk situations (e.g. for PEFPs, obtain senior management approval to keep account open after a determination has been made).

Step 6: Review Your Risk-Based Approach

Part of your risk assessment must also include a periodic review (minimum every 2 years) to test the effectiveness of your compliance regime, which includes:

- Your policies and procedures,
- Your risk assessment related to ML/TF, and
- Your training program (for employees and senior management).

This means that if your business model changes and new products or services are offered, your risk assessment should be updated along with your policies and procedures, mitigating measures and controls.

The review or your assessment of risks related to ML/TF has to cover all components, including your policies and procedures on risk assessment, risk mitigation and enhanced ongoing monitoring. This will help evaluate the need to modify existing policies and procedures or to implement new ones. As stated before, a risk-based approach is not a static exercise. The risks that you have identified will change or evolve over time as new products or new threats enter your business context. Consequently, the adherence and completion of this step is crucial to the implementation of an effective RBA.

☑ For more information, please consult section 8 of *Guideline 4: Implementation of a Compliance Regime*.

Here are a few examples/processes (using transaction testing) that your business could go through in order to review certain clients/businesses, in order to ensure that your compliance regime is effective.

Please note that these are **examples that are more specific to the review of your risk assessment.**

Examples:

1- Select a sample of cash intensive clients/businesses. From the sample selected, perform the following:

- Review account opening documentation including client identification and a sample of transaction activity;
- Determine if all applicable transactions have been reported to FINTRAC;
- Determine whether the actual account activity is consistent with the anticipated account activity;
- Look for trends in the nature, size, or scope of the transactions, paying particular attention to cash transactions;
- Determine whether ongoing monitoring is sufficient to identify suspicious activity; and
- Determine if the risk level for your client is appropriate or if it should be modified.

2- Evaluate your overall business risks related to funds transfer activities by analyzing the frequency and dollar volume of funds transfers in relation to your business size, its location, and the nature of your customer account relationships. Then select a sample of clients/businesses that utilize your electronic funds transfer services. From the sample selected, perform the following:

- Determine if all applicable transactions have been reported to FINTRAC;
- Determine whether the actual account activity is consistent with the anticipated account activity;
- Determine whether your suspicious activity monitoring and reporting system includes:
    - Identification of funds transfers purchased with cash;
    - Identification of transactions in which your business is acting as an intermediary;

    - Identification of transactions in which your business is sending or receiving funds transfers from foreign financial institutions, particularly to or from jurisdictions with strict privacy and secrecy laws or those identified as high-risk jurisdictions; and
    - Identification of frequent cash deposits and subsequent transfers, particularly to a larger institution or out of the country.
- Determine if the risk level for your client is appropriate or if it should be modified.

These examples highlight the importance of performing transaction testing as part of your review. Transaction testing can be done by the internal/external auditor or as part of your self-review. It will ultimately help your business determine if the policies and procedures, RBA and training are adequate and effective.

FINTRAC expectations for Step 6 – Review your risk-based approach:

As part of Step 6, FINTRAC expectations are that:

- A review is conducted at a minimum every two years or if there are changes in your business models, acquisition of a new portfolio, etc.

- The review covers your compliance policies and procedures, your assessment of risks related to ML/TF (i.e. your risk assessment) and your training program to test their effectiveness.

- The review must be documented and, within 30 days, be reported to senior management.

- The results of the review must also be documented, along with corrective measures and follow-up actions.

ANNEX A

References

FATF:

http://www.fatf-gafi.org/
http://www.fatf-gafi.org/documents/riskbasedapproach/

Statutory / Regulatory References:

http://laws-lois.justice.gc.ca/eng/acts/P-24.501/

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-317/

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-184/

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-121/

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/

Guideline 1: Backgrounder:
http://www.fintrac-canafe.gc.ca/publications/guide/Guide1/1-eng.asp

Guideline 2: Suspicious Transactions (includes ML/TF indicators):

http://www.fintrac-canafe.gc.ca/publications/guide/Guide2/2-eng.asp

Guideline 4: Implementation of a Compliance Regime:

http://www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp

Guideline 6: Record Keeping and Client Identification:

http://www.fintrac-canafe.gc.ca/publications/guide/Guide6/6-eng.asp

Assessment of Inherent risks of Money Laundering and Terrorist Financing in Canada:
http://www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp

ANNEX B

Example of risk segregation for a business-based risk assessment

As an example, the table below lists **some** risk factors that you could encounter **as part of your business-based risk assessment**. It also provides a rationale as to how you could differentiate between different risk ratings.

Please note that the PCMLTFA and Regulations do not require you to use a low, medium, high scale. You could decide to segregate between low and high risk categories only. A scale of risk must be established and, as noted earlier, must be tailored to your business's size and type.

Please note that utilizing a table similar to this one **is not** in itself an RBA as it does not meet the requirement as stated in the Regulations. The table below only outlines an example of a business-based risk assessment and does not consider your clients or business relationships.

☑ This list represents some **inherent risk** factors that have not been mitigated yet.

☑ By law, controls or mitigation measures will be required for all factors you identify as "high".

Factors	Low	Medium	High
Products & Services - Electronic Transactions	No electronic transaction services	You have some electronic transaction services and offer limited products and services	You offer a wide array of electronic transactions services
Products & Services - Currency Transactions	Few or no large currency transactions	Medium volume of large currency transactions	Significant volume of large currency or structured transactions
Products & Services – Funds Transfers	Limited number and value of funds transfers for clients, non-clients, limited third party transactions and no foreign funds transfers	Medium number and value of funds transfers, few international funds transfers from personal or business accounts with typically low-risk countries	Frequent and high value of funds transfers from personal or business accounts to or from high-risk jurisdictions and financial secrecy jurisdictions
Products & Services (business model) - International Exposure	Few international accounts or very low volume of currency activity in accounts	Medium level of international accounts with unexplained currency activity	Large number of international accounts with unexplained currency activity
Geography (location) - Prevalence of Crime	All my locations are in an area known to have a low crime rate	One or some of my locations are located in an area known to have a	One or some of my locations are located in an area known to have a high crime rate and/or

		medium crime rate	criminal organization(s)
Geography (high-risk countries)	No transactions with high-risk countries	Moderate volume of transactions with high-risk countries	Significant volume of transactions with high-risk countries

Note: Some of the descriptors in the above table could be interpreted as vague (e.g. “some”, “significant”, etc.); however, a table such as this one would have to be customized to the reality of your business.

For example, if FINTRAC states that a “significant volume of transactions with high risk countries” is considered high-risk, then one should compare the transactions to high-risk countries to the overall quantity of transactions conducted by the business. If the business conducts 1,000 transactions monthly and 600 of them are to high risk-countries; one could argue that it is “significant”.

The qualifiers must be applied to the specifics of your own business.

ANNEX C

Likelihood and Impact Matrix

For your business risks and/or client risks, you may want to use the likelihood and impact matrix described below. It is a visual tool that you can use to help determine the level of effort or monitoring required for the identified inherent risks. Note: the matrix below is an example only. As such, you can develop your own likelihood and impact matrix to better reflect the realities of your business.

1- Likelihood: Likelihood of an ML/TF risk (i.e. threat and vulnerability) occurring in your business.

- The chance of the risk being present = **likelihood**

☑ Ask yourself: What is the likelihood that the risks identified are actually present?

☑ The "likelihood" referred here is actually the level of risk you have identified as part of your business-based risk assessment and/or relationship-based risk assessment (e.g. a client assessed as medium risk).

You can use a scale similar to this one:

Rating	**Likelihood of ML/TF risk**
High	High probability that the risk is present
Medium	Reasonable probability that the risk is present
Low	Unlikely that the risk is present

2- Impact: The impact, on the other hand, refers to the seriousness of the damage (or consequence) that would occur if the assessed risk materialized.

- The damage/loss if the risk occurs = **impact**

Depending on business circumstances, the impact is the consequence of an ML/TF risk that can be looked at from the point of view of:

- Reputational risk and the impact on your business;
- Regulatory impact;
- Financial loss for your business;
- Legal risks;
- Other.

☑ The impact is in reference of an occurrence of ML/TF. The impact will be specific to each entity which makes it difficult to quantify. It will be up to the entity to determine the impact of its own risks.

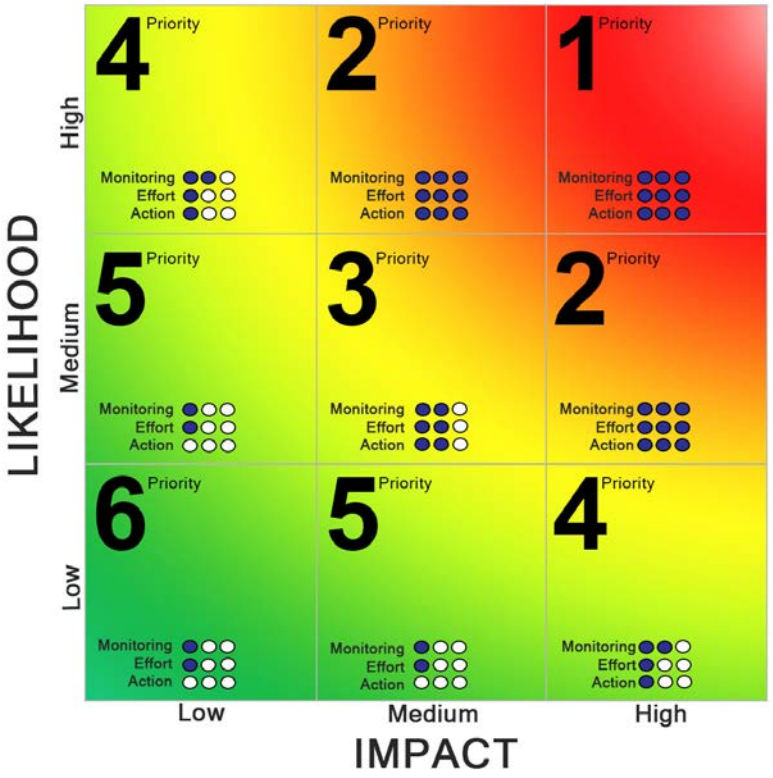
You can use a scale similar to this one:

Rating	Consequence of the ML/TF risk
High	The risk has severe consequences
Medium	The risk has moderate consequences
Low	The risk has minor or no consequences

When put together, the matrix can be used to help in deciding which action to take when the overall risk is considered. As stated before, a risk-based approach is a process that allows you to apply measures that are commensurate with the risks identified as part of your assessment.

Each box within the matrix outlines the level of resources required for:

- Action (i.e. the need to respond to the risk)
- Effort (i.e. level of effort required to mitigate the risk)
- Monitoring (i.e. level of monitoring required)



How to read the matrix:

Box #6 may not require any response, effort or monitoring due to the fact that you consider both the likelihood and impact to be low.

Box #3 will require you to allocate resources for action, effort and monitoring. You will want to monitor all business risks/business relationships that are in box #3 to ensure that the risks identified do not move into the red categories (boxes #1 and #2).

In Box #1, you have identified the risks to be highly likely with a severe impact on your business. Obviously, anything in this box (i.e. business risks, business relationship, etc.) would require the highest level of resources for action, effort and monitoring.

Examples:

As a business, you consider all risk factors or clients as:

- Low-risk if situated in boxes 5-6
- Medium-risk if situated in boxes 3-4
- High-risk if situated in boxes 1-2

Example #1

You complete the assessment of clients A & B and you determine that they both have the same likelihood for ML/TF: medium.

Taking a closer look at their accounts, you realize that both have wire transfers on file (product/service with a high inherent risk). However, client A has not conducted a wire in months and you also know that the wires were to family members abroad. Client B, however, regularly conducts wires but your knowledge of the recipients or the reasons for the wire transfers is minimal.

As such, you could assess the potential impact (or consequence) of ML/TF activities to be greater with client B than with client A. You could then decide to leave client A in the medium impact category (placing the client in the box #3) whereas client B could be moved to the high-impact category (placing the client in box #2).

As a result, you would need to implement mitigation measures for client B, now a high-risk client.

Example #2:

After completing the assessment of clients A & B, you determine that they have the same likelihood for ML/TF: high.

Taking a closer look at the volume of transactions they both conduct, you realize that client A conducts 1 transaction per week on average, whereas client B conducts several transactions every day. In this example, the impact (or consequence) of a few STR indicators and not submitting reports would be greater with client B because of the volume of transactions.

You could decide to place client A in a lower category (placing the client in box #4) whereas client B could remain in the higher category (placing the client in box #1 or #2).

As a result, you would implement mitigation measures for client B, now a high-risk client.

Example #3

Here is a scenario where the entity applies the risk matrix to risk elements that were identified as part of the risk assessment:

Risk Factor	Likelihood	Impact	Overall	Mitigation Measures
Clients always use cash as primary method of payments	High	Medium	**High (box #2)**	• Perform enhanced ongoing monitoring of transactions or business relationships • Obtain additional information beyond the minimum requirements about the intended nature and purpose of the business relationship, including the type of business activity
Clients frequently use wire transfers for no apparent reasons	Medium	High	**High (box #2)**	• Set transaction limits for high-risk products such as wire transfers to high-risk jurisdictions • Obtain additional information beyond the minimum requirements about the intended nature and purpose of the business relationship, including type of business activity • Implement a process to end an existing high-risk relationship which management sees as exceeding your risk tolerance level