Risk assessment guidance

> This guidance has been updated to include legislative amendments from June 2017 and legislative amendments that will come into force on June 1, 2021.

January 2021

FINTRAC developed this guidance to help you understand, as a reporting entity (RE):

- the types of money laundering (ML) and terrorist financing (TF) risks that you may encounter as a result of your business activities and clients; and
- what is a risk-based approach (RBA) and how you can use one to conduct a risk assessment of your business activities and clients.

This guidance also provides tools that you can use to develop and implement mitigation measures to address high-risk areas identified through your risk assessment. You can use these tools or you can develop your own risk assessment tools. This guidance is applicable to all REs subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, **some risk assessment obligations and/or examples may only apply to certain sectors**.

As part of your compliance program requirements under the PCMLTFA and associated Regulations, you must conduct a risk assessment of your ML/TF risks. [1] You are responsible for completing and documenting your own risk assessment. For more information about your risk assessment obligations see FINTRAC's Compliance program requirements guidance.

This guidance answers the following questions:

1. What is risk?
2. What are inherent and residual risks?
3. What is an RBA?
4. What is the RBA cycle?

It also contains the following annexes, which provide additional references, examples and tools to help you develop your RBA:

- Annex 1 — FINTRAC's RBA expectations
- Annex 2 — Examples of higher risk indicators and considerations for your business-based risk assessment
- Annex 3 — Examples of risk segregation for your business-based risk assessment
- Annex 4 — Likelihood and impact matrix
- Annex 5 — Examples of higher risk indicators and considerations for your relationship-based risk assessment

1. What is risk?

Risk is the likelihood of a negative occurrence or event happening and its consequences. In simple terms, risk is a combination of the chance that something may happen and the degree of damage or loss that may result. In the context of ML/TF, risk means:

- **At the national level:** Threats and vulnerabilities presented by ML/TF that put the integrity of Canada's financial system at risk, as well as the safety and security of Canadians. For example, organized crime groups operating in Canada that launder the proceeds of crime.
- **At the RE level:** Internal and external threats and vulnerabilities that could open an RE up to the possibility of being used to facilitate ML/TF activities. For example, a possible ML/TF risk at the RE level could be conducting business with clients located in high-risk jurisdictions or locations of concern.

Threats: A person, group or object that could cause harm. In the ML/TF context, threats could be criminals, third parties facilitating ML/TF, terrorists or terrorist groups or their funds.

Vulnerabilities: Elements of a business or its processes that are susceptible to harm and could be exploited by a threat. In the ML/TF context, vulnerabilities could include weak business controls or high-risk products or services.

2. What are inherent and residual risks?

Inherent risk is the risk of an event or circumstance that exists before you implement controls or mitigation measures. [2] Whereas residual risk is the level of risk that remains after you have implemented controls or mitigation measures.

When assessing risk, it is important to distinguish between inherent risk and residual risk. The RBA described in this guidance focuses on the inherent risks to your business, its activities and clients.

3. What is an RBA?

An RBA is a way for you to conduct your risk assessment by considering elements of your business, clients and/or business relationships to identify the impact of possible ML/TF risks, and to apply controls and measures to mitigate these risks.

The Financial Action Task Force (FATF), has developed a series of Recommendations that are recognized as the international standard for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. Recommendation 1 on the RBA, recognizes that an RBA is an effective way to combat money laundering and terrorist financing.

Using an RBA will enable you to:

- conduct a **risk assessment** of your business activities and clients taking into consideration certain elements, including:
  - your products, services and delivery channels [3];
  - the geographic location of your activities [4];
  - new developments and technologies [5];
  - your clients and business relationships [6];
  - the activities of your foreign and domestic affiliates [7] — This only applies to you if you are a financial entity, life insurance company or securities dealer, and the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer; and
  - any other relevant factor [8].
- **mitigate the risks you identify** through the implementation of controls and measures tailored to these risks, which includes the ongoing monitoring of business relationships for the purpose of:
  - keeping **client identification** information and, if required, beneficial ownership and business relationship information up to date in accordance with the assessed level of risk; [9]
    reassessing the level of risk associated with transactions and activities; [10]and

    - applying **enhanced or special measures** to those transactions and business relationships identified as high-risk. [11]
- identify and assess potential gaps or weaknesses of your compliance program. For example, using an RBA can help you to identify and assess risks that could impact other parts of your compliance program, such as gaps in your written policies, procedures or training program.

The PCMLTFA and associated Regulations do not prohibit you from having high-risk activities or high-risk business relationships. However, it is important that if you identify high-risk activities or high-risk business relationships that you document and implement appropriate controls to mitigate these risks and apply prescribed special measures.

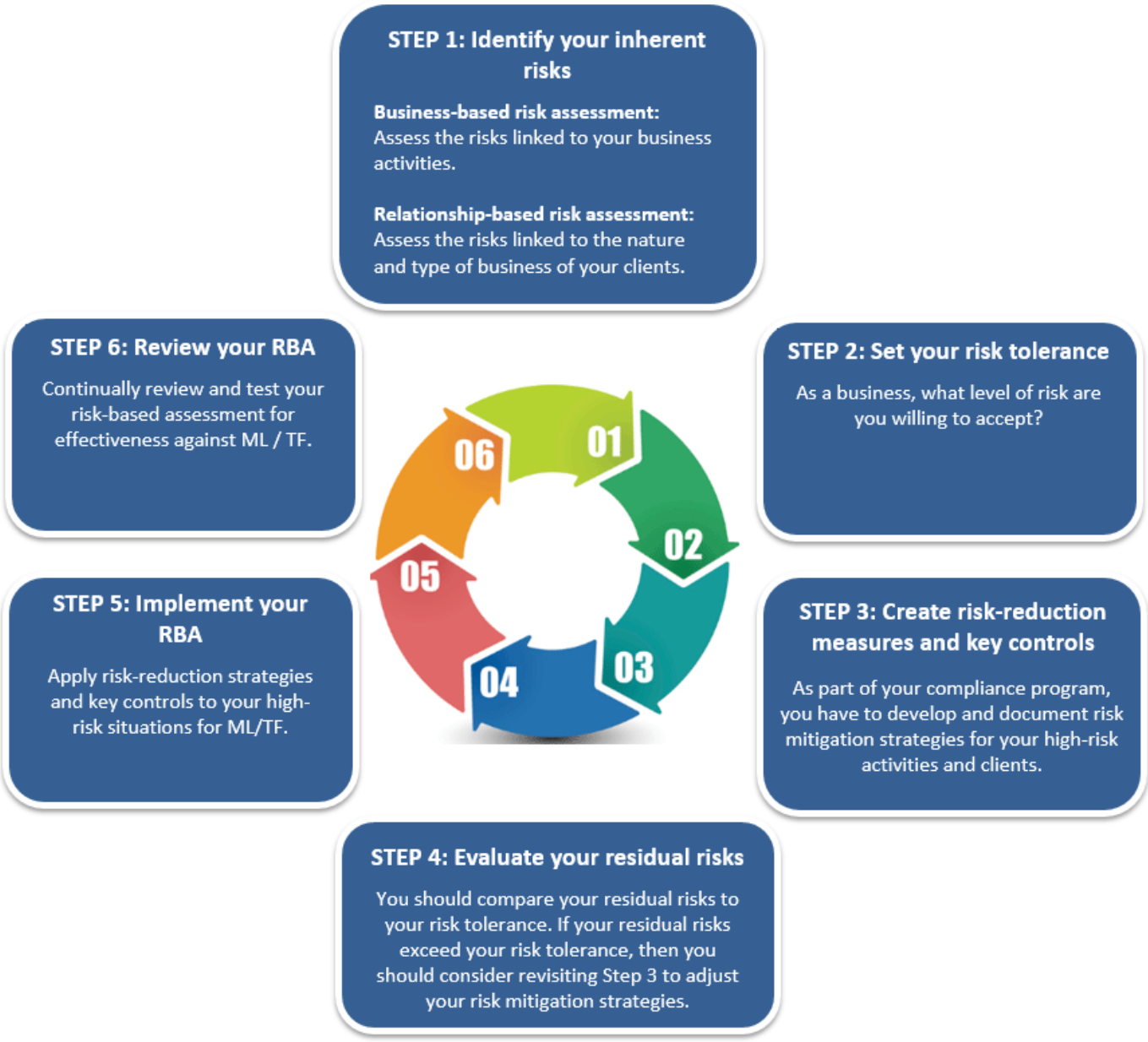
It is important to remember that assessing and mitigating the risk of ML/TF is not a static exercise. The risks you identify may change or evolve over time as new products, services, affiliations, or developments and technologies enter your business or its environment. You should be regularly reassessing the ML/TF-related risks to your business, and documenting that assessment to keep it up to date. For example, if you add a new product, service or technology to your business, or open a new location, you should evaluate and document the associated risks of this change to your business.

4. What is the RBA cycle?

The RBA cycle consists of six steps to follow to complete a risk assessment. The diagram below summarizes the RBA cycle. Additional information on how to conduct each step can be found further below.

It is important to note that there is no prescribed methodology for the assessment of risks. FINTRAC's suggested model presents business-based and relationship-based risk assessments separately. Although presented separately in this guidance, you can complete business-based and relationship-based assessments simultaneously. You will need to adapt this model to your business should you choose to use it.

Diagram 1: RBA cycle



RBA cycle — Step 1: Identify your inherent risks of ML/TF

To identify your inherent risks of ML/TF, you would start by assessing the following areas of your business:

- products, services and delivery channels;
- geography;
- new developments and technologies;
- clients and business relationships;
- activities of foreign and domestic affiliates, if applicable; and
- any other relevant factors.

Business-based risk assessment

Begin your risk assessment by looking at your business as a whole. This will allow you to identify where risks occur across business lines, clients or particular products or services. You will need to document mitigation controls for the areas you identify as high-risk. [12] The number of risks you identify will vary based on the type of business activities you conduct and products and/or services you offer.

To conduct a business-based risk assessment, you need to identify the inherent risks of your business by assessing your vulnerabilities to ML/TF. Your overall business-based risk assessment includes the risk posed by the following:

1. The combination of your products, services and delivery channels;
2. The geographical locations in which your business operates;
3. The impact of new developments and technologies that affect your operations;
4. The risks that result from affiliates (the activities that they carry out); and
5. Other relevant factors.

1. Products, services and delivery channels

You need to identify the products, services and delivery channels or ways in which they combine that may pose higher risks of ML/TF. Delivery channels are mediums through which you offer products and/or services to clients, or through which you can conduct transactions. See Annex 2 — Table 1: Business-based examples of higher risk indicators and considerations for products, services and delivery channels.

2. Geography

You need to identify the extent to which the geographic locations where you operate or undertake activities could pose a high-risk for ML/TF. Depending on your business and operations, this can range from your immediate surroundings, whether rural or urban, to a province or territory, multiple jurisdictions within Canada (domestic) or other countries. See Annex 2 — Table 2: Business-based examples of higher risk indicators and considerations for geography.

3. New developments and technologies

You need to identify the risks associated with new developments and the adoption of new technologies within your business. That is, if your business intends to put in place a new service/activity/location or introduce a new technology, then you must assess it in order to analyze the potential ML/TF risks it may bring to your business, before you implement it. See Annex 2 — Table 3: Business-based examples of higher risk indicators and considerations for new developments and technologies.

4. Foreign and domestic affiliates

If you are a financial entity, life insurance company or securities dealer, you need to identify the risks associated with having foreign and domestic affiliates, if the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer. An entity is your affiliate if one of you is wholly owned by the other, you are both wholly owned by the same entity, or your financial statements are consolidated. See Annex 2 — Table 4: Business-based examples of higher risk indicators and considerations for foreign and domestic affiliates.

5. Other relevant factors (if applicable):

You need to identify other factors relevant to your business and that could 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

See Annex 2 — Table 5: Business-based examples of higher risk indicators and considerations for other relevant factors.

Scoring your business-based risk assessment

Once you have identified and documented all the inherent risks to your business, you can assign a level or score to each risk using a scale or scoring methodology tailored to the size and type of your business. For example, very small businesses engaged in occasional, straightforward transactions may only require distinguishing between low and high-risk categories. FINTRAC expects larger businesses to establish more sophisticated risk scales or scoring methodologies, which could include additional risk categories.

By law, you must apply and document special measures for the high-risk elements of your business. [13] You must also be able to demonstrate to FINTRAC that you have put controls and measures in place to address these high-risk elements (for example, in your policies and procedures or training program), and that they are effective (this could be done through your internal or independent review). See Annex 3 — Table 6: Examples of risk segregation for a business-based risk assessment.

Additionally, you can use a likelihood and impact matrix tool similar to the one provided in Annex 4, to help you evaluate your business-based risk assessment.

Business-based risk assessment worksheet

Using a business-based risk assessment worksheet could be an easy way to document the inherent risks related to your business. The worksheet below is given as an example. You can also develop your own worksheet or method to document the inherent risks related to your business.

Diagram 2: Business-based risk assessment worksheet

Column A: **List of factors** **Identify all the risk factors that apply to your business (including, products, services and delivery channels, geography, new developments and technologies, foreign and domestic affiliates and other relevant factors)**	**Column B:** **Risk rating** **Assess each risk factor (for example, low, medium or high).**	**Column C:** **Rationale** **Explain why you assigned a particular risk rating to each risk factor.**
• High turnover within your business of employees who deal directly with clients.	High-risk	New employees may have less knowledge of certain clients and less experience with ML/TF indicators.
• Proximity to border crossings	High-risk	Your business may be the first point of entry into the local financial system.

Relationship-based risk assessment

Once you complete your business-based risk assessment, you can focus on the last element of your risk assessment, which consists of your clients and the business relationships you have with them.

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. [14] You also have to review this information on a periodic basis, which will help you determine the risk of ML/TF and understand the patterns and transactional activity of your clients. [15] It is possible that your business deals with clients outside of business relationships. The interactions with these clients may be sporadic (for example, few transactions over time that are under the identification threshold requirement). As such, there will not be a lot of information available to assess these clients. The risk assessment of such clients may focus on the transactional or contextual information at your disposal, rather than on a detailed client file.

If you do not have business relationships, it is not necessary for you to complete a relationship-based risk assessment worksheet for low and medium risk clients. However, if you have high-risk clients outside of business relationships, you should include them in a relationship-based risk assessment. For example, clients that were included in a suspicious transaction report (STR) you submitted to FINTRAC.

To conduct a relationship-based risk assessment, you need to identify the inherent risks of ML/TF for your clients. You can assess the ML/TF risks for individual clients or for groups of clients with similar characteristics. Your overall relationship-based risk assessment includes the risk posed by the following:

1. The combination of products, services and delivery channels your client uses;
2. The geographical location of the client and their transactions;
3. The new developments and technologies you make available to your clients; and
4. Client characteristics and patterns of activity or transactions.

1. Products, services and delivery channels

In the relationship-based risk assessment, you are looking at the products, services and delivery channels that your clients are using and the impact they have on your clients' overall risk.

Product risks:

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

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

Service risks:

You should include in your risk assessment services that have been identified as potentially posing a high-risk by government authorities or other credible sources.

For example, potentially higher risk services could include: international electronic funds transfers (EFTs), international correspondent banking services, international private banking services, services involving banknote and precious metal trading and delivery, or front money accounts for casinos.

Delivery channel risks:

You should consider delivery channels as part of your risk assessment, given the potential impact of new developments and technologies.

Delivery channels that allow for non-face-to-face transactions pose 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, chat applications, online document signing, etc.)

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 therefore poses a higher risk. Although some delivery channels may have become the norm (for example, the use of internet for banking), you should nonetheless consider them in combination with other factors that could make a specific element, client or group of clients high-risk.

Some products, services and delivery channels inherently pose a higher risk. See Annex 5 — Table 9: Relationship-based examples of higher risk indicators and considerations for products, services and delivery channels.

2. Geography

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

Your business faces increased ML/TF risks when you receive funds from or destined to high-risk jurisdictions, and when a client has a material connection to a high-risk country. You should assess the risks associated with your clients and business relationships such as residency in a high-risk jurisdiction or transactions with those jurisdictions.

See Annex 5 — Table 10: Relationship-based examples of higher risk indicators and considerations for geography.

3. Impacts of new developments and technologies

In the business-based risk assessment, you assessed potential high-risk elements related to the introduction of new developments and technologies in your business model, prior to implementing them. In the relationship-based risk assessment, you will examine the potential impacts that new developments (putting in place a new service/activity/location) and technologies (introducing a new technology) could have on your clients, affiliates, and anyone with whom you have a business relationship.

New developments and technologies can increase risk, as they may provide another layer of anonymity. For example, your business faces an increased risk of ML/TF when funds come from or are destined to high-risk jurisdictions, and when the origin of the funds can not be determined or is unknown, etc.

See Annex 5 — Table 11: Relationship-based examples of higher risk indicators and considerations for new developments and technologies.

4. Client characteristics and patterns of activity or transactions

At the beginning of a business relationship, and periodically throughout the relationship, you should consider the purpose and intended nature of the relationship. Doing so will help you understand your clients' activities and transaction patterns, in order to determine their level of ML/TF risk. Your policies and procedures must reflect this process.

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** a client's overall ML/TF risk rating, such as:

- criminal history of the client in regards to a designated offence (See Guideline 1 — Section 2.1 for more details;
- unknown source of funds;
- beneficiary of the transaction is unknown;
- individual conducting the transaction in unknown;
- absence of detail in the transaction records;

- unusual speed, volume and frequency of transactions; or
- unexplained complexity of accounts or transactions.

Similarly, you should also look at factors that can **decrease** a client's ML/TF risk, such as:

- a low volume of activity;
- a low aggregate balance;
- low dollar value transactions; or
- household expense accounts or accounts for the investments of funds that are subject to a regulatory scheme (for example, Registered Retirement Savings Plan).

Some client characteristics or patterns of activity will pose an inherently higher risk of ML/TF. For examples of:

- higher risk client characteristics and patterns of activity, see Annex 5 — Table 12: Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity;
- client characteristics that can be considered higher risk, see FINTRAC's ML/TF indicators; and
- additional higher risk indicators and rationale, see Annex 5 — Table 13: Relationship-based examples of additional higher risk indicators and related considerations.

Scoring your relationship-based risk assessment

You can assess the ML/TF risk for individual clients or for groups of clients. This assessment could take the form clusters (or groups) of clients with similar characteristics. For example, you can group together clients with similar incomes, occupations and portfolios, or those who conduct similar types of transactions. This approach can be especially practical for financial institutions.

It is important to remember that identifying one high-risk indicator for a client does not necessarily mean that the client poses a high-risk (with the exception of the three indicators highlighted in Table 12). 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 activity. It is up to you to determine how to best assess the risk each client or group of clients poses.

Every high-risk client (or group of clients) will need to be subjected to prescribed special measures (see step 3). You will have to document these measures in your policies and procedures, and document how you apply them to your high-risk clients. [16]

You can use a Likelihood and impact matrix like the one in Annex 4 to help you evaluate your relationship-based risk.

Relationship-based risk assessment worksheet

Using a relationship-based risk assessment worksheet could be an easy way to document the inherent risks related to your clients and your business relationships with them. The worksheet below is given an example. You can also develop your own worksheet or method to document the inherent risks related to your clients.

Diagram 3: Relationship-based risk assessment worksheet

Column A **Business relationships and/or high-risk clients** **Identify all your business relationships and/or high-risk clients (individually or as groups).**	**Column B:** **Risk rating** **Rate each business relationship and/or client (or group of clients) (for example, low, medium or high risk).**	**Column C:** **Rationale** **Explain why you assigned that particular rating to each business relationship and/or client (or group of clients).**
• Group A / Client A	Low-risk	Known group or client conducting standard transactions in line with their profile.
• Group B / Client B	High-risk	Conducts several large cash transactions that seem to be beyond their means.

RBA cycle — Step 2: Setting your risk tolerance

Risk tolerance is an important component of effective risk management. Consider your risk tolerance before deciding how you will address risks. When considering threats, the concept of risk tolerance will allow you to determine the level of risk exposure that you consider tolerable.

To do so, you may want to consider the following types of risk which can affect your organization:

- regulatory risk;
- reputational risk;
- legal risk; or
- financial risk.

The PCMLTFA and associated Regulations state that reporting entities have obligations when they identify high-risk business activities and high-risk clients. Setting a high risk tolerance does not allow reporting entities to avoid these obligations.

To set your risk tolerance, some questions that you may want to answer are:

- Are you willing to accept regulatory, reputational, legal or financial risks?
- Which risks are you willing to accept after implementing mitigation measures?
- Which risks are you not willing to accept?

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

RBA cycle — Step 3: Creating risk-reduction measures and key controls

Risk mitigation is the implementation of controls to manage the ML/TF risks you have identified while conducting your risk assessment. It includes:

1. **In all situations,** your business should consider implementing internal controls that will help mitigate your overall risk.
2. **For your business-based risk assessment,** you will have to document and mitigate all the high-risk elements identified by your assessment with controls or measures. [17]
3. **For all your clients and business relationships**, you will be required to: [18]
    a. Conduct ongoing monitoring of all your business relationships; and
    b. Keep a record of the measures and information obtained through this monitoring.
4. **For your high-risk clients and business relationships**, you will be required to adopt the prescribed special measures, including: [19]
    a. Conducting **enhanced** monitoring of these clients and business relationships.
    b. Taking enhanced measures to verify their identity and/or keep client information up to date.

Implementing risk mitigation measures will allow your business to stay within your risk tolerance. It is important to note that having a higher risk tolerance may lead to your business accepting higher risk situations and/or clients. If you accept to do business in higher risk situations and/or with higher risk clients, you should have stronger mitigation measures and controls in place to adequately address the risks.

For **detailed** information on risk mitigation measures, please consult FINTRAC's Compliance program requirements guidance.

RBA cycle — Step 4: Evaluating your residual risks

Your residual risks should be in line with your risk tolerance. It is important to note that no matter how robust your risk mitigation measures and risk management program is, your business will always have exposure to some residual ML/TF risk that you must manage. If your residual risk is greater than your risk tolerance, or your measures and controls do not sufficiently mitigate high-risk situations or high-risk posed by clients, you should go back to step 3 and review the mitigation measures that were put in place.

If your business is willing to deal with high-risk situations and/or clients, FINTRAC expects that the mitigation measures or controls put in place (see step 3) will be commensurate with the level of risk, and that the residual risks will be reasonable and acceptable.

Types of residual risk:

- **Tolerated risks:** These are risks that you accept because there is no benefit in trying to reduce them. Tolerated risks may increase over time. For example, when you introduce a new product or a new threat appears.
- **Mitigated risks:** These are risks that you have reduced but not eliminated. In practice, the controls put in place may fail from time to time (for example, you do not report a transaction within the prescribed timeframe because your transaction review process has failed).

This is an example of a business further mitigating risk because over time their risks and clients have evolved:

Business A offers international EFTs as a service to its clients. Reporting systems are in place to capture transactions of $10,000 or more, and Business A has developed policies and procedures to properly verify identity for transactions of $1,000 or more. A reporting system is also in place to identify transactions that could be related to an ML/TF offence (for suspicious transaction reporting purposes).

Since Business A considers international EFTs 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 EFTs and are made aware of updates and changes

to high-risk jurisdictions as indicated in government advisories. These measures were put in place by Business A years ago and are well understood and followed by the staff.

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

However, as risks and/or clients changed over time, Business A now feels that the mitigation measures are no longer sufficient to meet its risk tolerance. In fact, Business A's risk tolerance is now lower than it used to be (that is, it is less inclined to take on high-risks). 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 additional mitigation measures are:

- put a limit on specific transactions (for example, international EFTs to specific jurisdictions);
- require additional internal approvals for certain transactions; and/or
- monitor some transactions more frequently to help reduce the risk of structuring (for example, a $12,000 transaction that is split into two $6,000 transactions to avoid reporting).

RBA cycle — Step 5: Implementing your RBA

You will implement your RBA as part of your day-to-day activities.

You must document your risk assessment as part of your compliance program. [20] A detailed and well-documented compliance program shows your commitment to preventing, detecting and addressing your organization's ML/TF risks.

Risk and risk mitigation requires the leadership and engagement of your senior management (should this apply to your business). Senior management or your business owner is ultimately accountable, and may be responsible for making decisions related to policies, procedures and processes that mitigate and control ML/TF risks.

For more information, please consult FINTRAC's Compliance program requirements guidance.

RBA cycle — Step 6: Reviewing your RBA

You must institute and document a periodic review (minimum of every two years) of your compliance program, to test its effectiveness, which includes reviewing: [21]

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

If your business model changes and you offer new products or services, you should update your risk assessment along with your policies and procedures, mitigating measures and controls, as appropriate.

When reviewing your risk assessment to test its effectiveness, you must cover all components, including your policies and procedures on risk assessment, risk mitigation strategies and special measures which include your enhanced ongoing monitoring procedures. This will help you evaluate the need to modify existing policies and procedures or to implement new ones. Consequently, the completion of this step is crucial to the implementation of an effective RBA.

For more information, please consult FINTRAC's Compliance program requirements guidance.

Annex 1 — FINTRAC's RBA expectations

Overall expectations

There is no standard risk assessment methodology. In building a new or validating an existing risk assessment, you may find this guidance useful to inform your risk assessment. However, you should not limit yourself to the information provided in this guidance when developing your own RBA.

The expectations below are at a high level. FINTRAC's risk assessment expectations for each step of the RBA cycle are described further in this annex.

- Your risk assessment must be documented and should:
  - reflect the reality of your business;
  - include all prescribed elements (products, services and delivery channels, geography, new developments and technologies, affiliates if applicable, and any other factors relevant to your business); and
  - be shared with FINTRAC during an examination upon request.
- You need to tailor your risk assessment to your business size and type. For example, FINTRAC would expect a more detailed assessment from REs that conduct large volumes of transactions across various business lines and/or products. Additionally, FINTRAC would expect the overall business-based risk rating for larger REs to have separate risk ratings for different lines of business.
- You need to document all steps of your risk assessment, the process you followed, and the rationale that supports your risk assessment.
- During an examination, FINTRAC may review:
  - 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 assessed based on the products, services, delivery channels, geographical risk, impact of new developments and technologies and other characteristics or patterns of activities;
  - your high-risk client files to ensure that the prescribed special measures have been applied;
  - your records to assess whether monitoring and reporting are done in accordance with the PCMLTFA and associated Regulations and with your policies and procedures; and
  - whether your prescribed review (to be conducted at least once every two years) appropriately assessed the effectiveness of your business and relationship-based risk assessment.

Expectations for Step 1 — Identification of your inherent risks

FINTRAC expects that:

- You have considered and assessed your business risks (including, products, services and delivery channels, geography, new developments and technologies, affiliates if applicable, and any other factors relevant to your business) and you are able to provide a rationale for your assessment. For every element that you assess as posing a high-risk, you will need to document the controls and mitigation measures you are taking. You need to be able to show that these controls and measures have been implemented.
- You have considered and assessed your clients and business relationships based on the products, services and delivery channels they use, on their geography, and on their characteristics and patterns of activity. You can do this by:
  - Demonstrating that you have assessed the risks posed by each client you have a business relationship with; or
  - Assessing groups of clients or of business relationships that share similar characteristics, 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 in your assessment (such as those included in this guidance where applicable).
- In situations where high-risk indicators are not considered (for example, FINTRAC considers a specific element to pose a high-risk but you decide that the element poses a lower level of risk), you must be able to provide a reasonable rationale.
- For every high-risk relationship, you have put in place the prescribed special measures and document these measures in your policies and procedures.
- If you use a checklist for your risk assessment, you must be able to provide a documented analysis of the risk that draws conclusions on your business's vulnerabilities to ML/TF and the threats it faces, including the required elements (referred to above).
- If your business is using a service provider to perform the risk assessment, you are nonetheless ultimately responsible to ensure that the for the risk assessment obligation is met correctly.

Expectations for Step 2 — Set your risk tolerance

FINTRAC expects that:

- You take time to establish your risk tolerance, as it is an important component of effectively assessing and managing your risks.
- Your risk tolerance will have a direct impact on creating risk-reduction measures and controls, on your policies and procedures, and on training (step 3).

Setting your risk tolerance includes obtaining approval from senior management (should that be a part of your business structure).

Expectations for Step 3 — Create risk-reduction measures and key controls

FINTRAC expects that:

- You keep the client identification and beneficial ownership information of your business relationships up to date. [22]
- You establish and conduct the appropriate level of ongoing monitoring for your business relationships (taking enhanced measures for high-risk clients). [23]
- You implement mitigation measures for situations where the risk of ML/TF is high (for your business-based risks and relationship-based risks). These written mitigation strategies must be included in your policies and procedures.

Apply your controls and procedures consistently. FINTRAC may assess them through transaction testing.

Expectations for Step 4 — Evaluate your residual risks

FINTRAC expects that:

- You take the time to evaluate your level of residual risk.
- You confirm that the level of residual risk is aligned with your risk tolerance (as described in step 2).

Expectations for Step 5 — Implement your RBA

FINTRAC expects that:

- Your RBA process is documented, and includes your ongoing monitoring procedures (including their frequency) and the measures and controls put in place to mitigate the high-risks identified in step 1.
- You apply your RBA as described in your documentation.
- You keep the client and beneficial ownership information of your business relationships up to date. [24]
- You conduct ongoing monitoring of all your business relationships. [25]
- You apply the appropriate prescribed special measures to your high-risk clients and business relationships. [26]
- You involve the persons responsible for compliance when dealing with high-risk situations (for example, when dealing with foreign politically exposed persons (PEPs), obtain senior management approval to keep accounts open after a determination has been made).

Expectations for Step 6 — Review your RBA

FINTRAC expects that:

- You conduct a review at least every two years, or when there are changes to your business model, when you acquire a new portfolio, etc. [27]
- This prescribed review will test the effectiveness of your entire compliance program, including your compliance policies and procedures, your risk assessment of ML/TF risks and your ongoing training program. [28]
- You document the review and report it to senior management within 30 days. [29]
- You document the results of the review, along with corrective measures and follow-up actions. [30]

Annex 2 — Examples of higher risk indicators and considerations for your business-based risk assessment

Table 1: Business-based examples of higher risk indicators and considerations for products, services and delivery channels

Examples of higher risk indicators	Considerations

Higher risk products and services, such as: • EFTs, • electronic cash (for example, stored value cards and payroll cards) • letters of credit • bank drafts • front money accounts • products offered through the use of intermediaries or agents • private banking • mobile applications	Legitimate products and services can be used to mask the illegitimate origins of funds, to move funds to finance terrorist acts or to hide the true identity of the owner or beneficiary of the product or service. You should assess the market for your products and services (for example, corporations, individuals, working professionals, wholesale or retail etc.), as this may have an impact on the risk. Do the products or services you provide allow your clients to conduct business or transactions with higher risk business segments? Could your clients use the products or services on behalf of third parties? Products and services offered that are based on new developments and technologies such as electronic wallets, mobile payments, or virtual currencies, may be considered higher risk as they can transmit funds quickly and anonymously.
Delivery channels, such as transactions for which an individual is **not physically present**, including • agent network • online trading	Your delivery channels may have a higher inherent risk if you offer non face-to-face transactions, use agents, or if clients can initiate a business relationship online. This is especially true if you rely on an agent (that may or may not be covered by the PCMLTFA) to verify the identity of your clients. For the purpose of the PCMLTFA, REs are accountable for the activities conducted by their agents. In addition, new delivery channels (for example, products or services such as virtual currency) may pose inherently higher ML/TF risks due to the anonymous nature of transactions when conducted remotely.

Table 2: Business-based examples of higher risk indicators and considerations for geography

Examples of higher risk indicators	Considerations

Border-crossings: • air (for example, airports) • water (for example, ports, marinas) • land (for example, land border-crossings) • rail (for example, passenger and cargo)	If your business is near a border-crossing, you may have a higher inherent risk because 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 clients as posing a high-risk if your business is located near a border-crossing or major airport. FINTRAC is simply highlighting that such businesses may want to pay closer attention to the fact that their geographical location may impact their business. For example, this could be done through training so that staff better understand the placement stage of ML and its potential impacts.
Geographical location and demographics: • large city • rural area	Your geographical location may also affect your overall business risks. For example, a rural area where you know your clients 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 on crime by regions, which may inform your risk assessment, such as Québec (http ://geoegl.msp.gouv.qc.ca/dpop/) (in French only). Other websites provide good information on crime in Canada, including statistics and trends by province. For example, crimes, by type of violation, and by province and territory: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/legal50b-eng.htm.

Your business is located in an area known for having a high crime rate	High crime rate areas should be indicated in the overall assessment of your business as they may present higher ML/TF risks. You do not need to consider every client from a higher crime area as posing a high-risk. However, you should be aware of how these areas can affect client activities. Searching online for crime related statistics in your city or area should result insources you can consult (such as municipal police departments or other databases). For example, the following websites provide information on crime in cities or neighborhoods: • 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: https://winnipeg.ca/police/crimestat/viewMap.aspx • Toronto: http://www.torontopolice.on.ca/statistics/stats.php • Ottawa: https://www.ottawapolice.ca/en/crime/crime-stats.aspx • Montreal: https://ville.montreal.qc.ca/vuesurlasecuritepublique/ (in French only) • Halifax: https://www.halifax.ca/fire-police/police/crime-mapping Please note that statistics such as those found under the links above are not necessarily linked to ML/TF offences. They provide a general idea of where crime occurs in a given city.
Events and patterns	Depending on your clientele, are there events or patterns (either domestic or international) that could affect your business? For example, you may be dealing with clients that have a connection to high-risk jurisdictions or with jurisdictions that are dealing with a specific event (such as terrorism, war, etc.). You do not need to classify all activities and clients as posing a high-risk in relation to an event, conflict or high-risk jurisdiction. However, you should be aware of these circumstances in order to determine whether a transaction becomes unusual or suspicious.

Connection to high-risk countries: • Special Economic Measures Act (SEMA) • FATF list of High-Risk Countries and Non-Cooperative Jurisdictions • UN Security Council Resolutions • Freezing Assets of Corrupt Foreign Officials Act (FACFOA) sanctions	International conventions and standards may affect mitigation measures aimed at the detection and deterrence of ML/TF. You should identify certain countries 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 ML/TF control regime, or the fact that they are listed in the advisories of competent authorities such as the FATF or FINTRAC. If you and/or your clients have no connection to these countries, the risk will likely be low or non-existent. If you transfer funds to or receive funds from a country subject to economic sanctions, embargoes or other measures, you should consider that country as high-risk. For example, you should be aware of: • Canadian Economic Sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng • 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/1-eng.asp • Security Council Resolutions: https://www.un.org/securitycouncil/content/resolutions-0 • Freezing Assets of Corrupt Foreign Officials Act sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng

Table 3: Business-based examples of higher risk indicators and considerations for new developments and technologies

Examples of higher risk indicators	Considerations
Use of technology, such as: • Payment methods: ◦ E-wallets in fiat currencies	Your overall inherent risks may be higher if your business adopts new technologies or operates in an environment subject to frequent technological change. New technologies may include systems or software used in your organizations ML/TF mitigation strategy such as a transaction monitoring system or a client onboarding or identification tool.

(CAD, USD, etc.) ◦ E-wallets in virtual currencies ◦ pre-paid cards ◦ internet payment services ◦ mobile payments ◦ money transfers between individuals over mobile devices and the Internet • Methods of communication or identification: ◦ phone ◦ email ◦ chat applications ◦ electronic information exchange ◦ document signing on a cloud server such as DocuSign	The implementation of new technologies such as mobile payment services could subject your business to a wide range of vulnerabilities that can be exploited for ML. For example, the use of new technologies can result in less face-to-face interaction with customers, allowing more anonymity and possibly increasing ML/TF risks. Therefore, when you implement new technology in your business, it is important that you assess the associated ML/TF risks and document and implement appropriate controls to mitigate those risks. **Payment methods** The payment method examples listed in the Indicators column can be used to transfer funds faster and anonymously, which can increase ML/TF risks. If your business offers such products, services and delivery channels, you must assess them for ML/TF risks to your business. **Methods of communication or identification** Your business may communicate with clients through means other than the telephone and email or your clients may use new ways to communicate with you or identify themselves to you. Communications means are evolving continually and can affect your overall inherent risks.
New developments	Consider acquisitions, changes to your business model, or business restructuring.

Table 4: Business-based examples of higher risk indicators and considerations for foreign and domestic affiliates

Examples of higher risk indicators	Considerations
Business model of foreign affiliate: • operational structure • reputational risk	Review the business model, size, number of employees and the products and services of your affiliates to determine whether they represent a risk that can affect your business. For example: • If a business has hundreds of branches and thousands of employees, it poses different risks than a business with a single location and two employees. • If the media negatively mentions one of your affiliates, your reputation could also be affected given the connection between you and that affiliate.

Table 5: Business-based examples of higher risk indicators and considerations for other relevant factors

Examples of higher risk indicators	Considerations
• Special Economic Measures Act (SEMA) • ministerial directives • regulators • national risk assessment	Restrictions such as economic 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, regions, non-state actors (such as terrorist organizations), or designated persons from a target country. As part of your risk assessment, you must also take into consideration ministerial directives. Your sector's regulator may also impose additional measures (for example, provincial, prudential, etc.). The national risk assessment 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 • ML/TF actors including organized crime groups, terrorist organizations, facilitators, etc. • corruption and other crimes	Trends and typologies for your respective activity sector may include specific elements of risks that your business should consider. For example: • FATF Methods and Trends (not available for all activity sectors): http://www.fatf-gafi.org/topics/methodsandtrends/). • Public Safety Canada — Organized Crime: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmbtng-rgnzd-crm/index-en.aspx • Transparency International (rank by country): https://www.transparency.org/country/# 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 partyand/or service providers	To determine if risks exist in relation to this element, you need to consider your business model, the size of your business, and the number of branches and employees. For example: • A business with hundreds of branches and thousands of employees will present different risks than a business that has one location and two employees. • A business with a high employee turnover. These examples highlight the fact that your risk assessment should be related to other compliance program elements, such as training. Training should give employees an understanding of the reporting, client identification, and record keeping requirements, and an understanding of the penalties for not meeting those requirements. If you have numerous branches or a high employee turnover, your training program should address these risks. 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 complying with your obligations under the PCMLTFA and associated Regulations. You will want to ensure that you fully understand how your third party or service provider is functioning.

Annex 3 — Examples of risk segregation for your business-based risk assessment

The table below lists examples of risk factors you could encounter **as part of your business-based risk assessment**. It also provides a rationale on how you could differentiate between risk ratings.

Please note that:

1. The PCMLTFA and associated Regulations do not require you to use a low, medium and high scale. You could use low and high-risk categories only. You must establish a risk scale and you must tailor the risk scale to your business's size and type.
2. Utilizing a table similar to this one **is not** in itself a risk assessment, as it does not meet the requirement as stated in the Regulations. However, the table below is an example of a business-based risk assessment. It does not consider your clients or business relationships.

This list includes **inherent risks** that have not been mitigated yet. By law, controls or mitigation measures are required for all high-risk factors.

Table 6: Examples of risk segregation for a business-based risk assessment

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 transactions	Medium volume of large transactions	Significant volume of large or structured transactions
Products & services — EFTs	Limited number of funds and transfers of low value for clients and non-clients Limited third party transactions and no foreign funds transfers	Regular funds transfers and transfers of medium value Few international funds transfers from personal or business accounts with typically low-risk countries	Frequent funds transfers and transfers of high value 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 transactions in international accounts	Some international accounts with unexplained transactions	High number of international accounts with unexplained transactions
Geography (location) — Prevalence of crime	All locations are in an area known to have a low crime rate	One or a few locations are in an area known to have an average crime rate	One or a few locations are in an area known to have a high crime rate and/or criminal organization(s)
Technology	No new technologies are used to conduct the business in terms of products and services to clients No new technologies are used to contact clients	Certain areas of the business use new technologies to contact clients but products, services and payment methods do not use new technologies	The majority of products, services, delivery channels, payment methods and client contact methods use new technologies.

Note: Some of the descriptors in the above table are vague (such as "some", "significant", etc.). A table such as this one needs to be customized to the reality of your business. For example, if FINTRAC states that it considers a "significant volume of transactions with high-risk countries" as posing a high-risk, this could mean that a business could compare the transactions to high-risk countries to the overall quantity of transactions conducted by their business. If a business conducting 600 transactions with high-risk-countries out of 1,000 monthly transactions it has a "significant" inherent risk. Qualifiers depend on the specifics of your own business.

Annex 4 — Likelihood and impact matrix

You can use the likelihood and impact matrix described below for your business and client risks. It can help you determine the level of effort or monitoring required for inherent risks. You use the matrix or develop your own to better reflect the realities of your business.

Likelihood is the chance of an ML/TF risk is present. What is the likelihood that the identified risks are actually present? The "likelihood" is the level of risk you have identified as part of your business-based risk assessment and/or your relationship-based risk assessment (for example, a client assessed as posing a medium risk). You can use a scale similar to this one:

Table 7: Rating and likelihood of the ML/TF risk

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

Impact is the damage incurred if ML/TF occurs. Depending on business circumstances, the impact could be a financial loss, or a regulatory, legal, reputational or other impact. To help you determine the impact of your ML/TF risks, you can use a scale similar to this one:

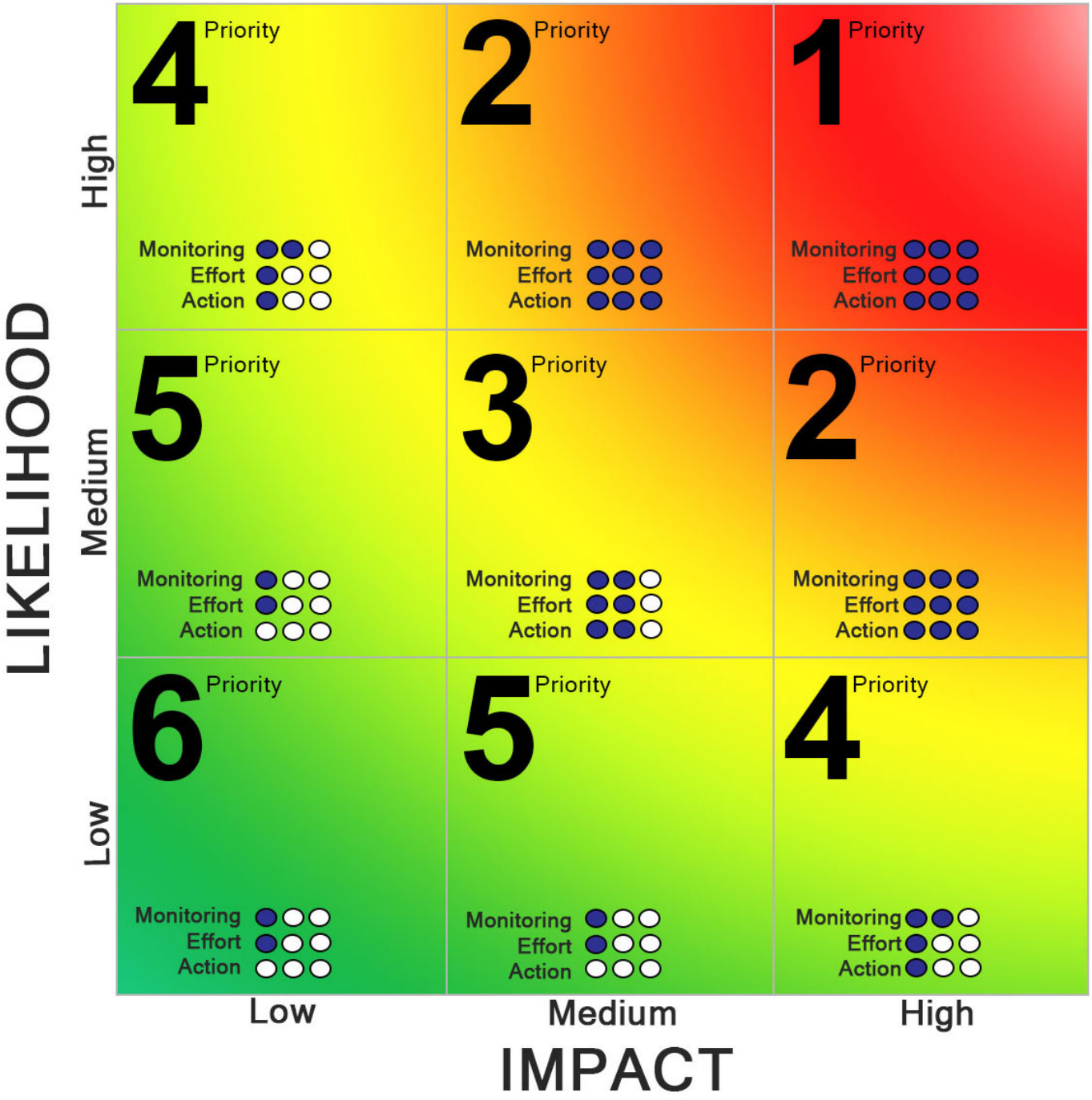
Table 8: Rating and impact of the ML/TF risk

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

You can use the matrix to help you decide which actions to take considering the overall risk. Each box in the matrix shows the level of resources required for:

- action (the need to respond to the risk)
- effort (level of effort required to mitigate the risk)
- monitoring (level of monitoring required)

Diagram 4: Likelihood and impact matrix



▶ View Text Equivelant

How to read the matrix

Box 6 may not require any response, effort or monitoring because 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 and 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 to occur and to have a severe impact on your business. Anything in this box (for example, business risks, business relationship, etc.) would require the most resources for action, effort, and monitoring.

Examples

For the example below, you should consider all risk factors or clients as:

- low-risk if situated in boxes 5–6;
- medium-risk if situated in boxes 3–4; and
- high-risk if situated in boxes 1–2.

Example 1

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

Taking a closer look at their accounts, you realize that both have EFTs on file (product/service with a high inherent risk). However, client A has not conducted an EFT in months and you know that the EFTs were to family members abroad. However, client B regularly conducts EFTs but you do not know a lot about the recipients or the reasons for the EFTs.

As such, you could assess the impact of the ML/TF risk to be greater with client B than with client A. You could decide to leave client A in the medium impact category (placing the client in box 3) and to move client B to the high-impact category (placing the client in box 2). You should document your decision and rationale.

In this example, you would need to implement mitigation measures for client B, who is now a high-risk client.

Example 2

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

Taking a closer look at the volume of transactions both clients conduct, you see that client A conducts 1 transaction per week on average; whereas client B conducts several transactions every day. In this example, the impact not submitting suspicious transaction 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) while client B could remain in a higher category (placing the client in box 1 or 2). You should document your decision and rationale

In this example, you would implement mitigation measures for client B, who is now a high-risk client.

Example 3

In this scenario, an RE applies the risk matrix to risk elements identified in their risk assessment:

Diagram 5 — Example of a risk matrix

Risk factor	Likelihood	Impact	Overall	Mitigation measures

Clients always use cash as method of payment	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 EFTs for no apparent reason	Medium	High	**High (box 2)**	• Set transaction limits for high-risk products such as EFTs to high-risk jurisdictions. • Obtain additional information beyond the minimum requirements for the intended nature and purpose of the business relationship, including type of business activity. • Implement a process to end existing high-risk relationships that exceed your risk tolerance level.

Annex 5 — Examples of higher risk indicators and considerations for your relationship-based risk assessment

Table 9: Relationship-based examples of higher risk indicators and considerations for products, service and delivery channels

Examples of higher risk indicators	Considerations
Your clients use electronic funds payment services such as: • EFTs • electronic cash	EFTs can be done in a non-face-to-face environment. Additionally, transmitting large amounts of funds outside of Canada or into Canada can disguise the origin of the funds. **Electronic cash** is a higher risk service because it can allow unidentified parties to conduct transactions.

Your clients use 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. They are much like cash in the sense that the holder of the draft is the owner of the money. For example, a 100,000 dollar bank draft (showing a financial institution as the payee) and can be passed from one person to another, effectively blurring the money trail. You can mitigate the inherent risk of this product when it is issued as payable only to specific payees and when the information about the draft's originator are included (name, account number, etc.). **Letters of credit** are essentially a guarantee from a bank that a seller will receive payment for goods. While guaranteed by a bank, letters of credit have a higher inherent ML/TF risk as they can be used in trade-based transactions to increase the appearance of legitimacy and reduce the risk of detection. Money launderers using trade-based transactions (for example, seller or importer) may also use under or over valuation schemes, which will allow them to move money under the veil of legitimacy. There is also higher risk when letters of credit are not used in a way 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 use intermediaries, agents or introducers (refer clients or businesses to you for specific products or services).	Non-face-to-face transactions can make it more difficult to verify the identity of your clients. Using intermediaries or agents may increase your inherent risks, because intermediaries or agents may lack adequate supervision if they are not subject to anti-money laundering and anti-terrorist financing (AML/ATF) laws or measures. It is important to note that under the PCMLTFA, you are accountable for the activities conducted by all your agents. As a result, you need to ensure that they meet all compliance obligations on an ongoing basis. Furthermore, you should have due diligence processes in place (such as background checks and ongoing monitoring) to lessen the risk of your agent network being used for ML/TF purposes.

Table 10: Relationship-based examples of higher risk indicators and considerations for geography

Examples of higher risk indicators	Considerations
Your client's proximity to a branch or location	A client that conducts business or transactions away from their home branch or address without reasonable explanation. For example, one of your clients conducts transactions at different branches across a broad geographical area over one day and this does not appear to be practical.
Your client is a non-resident	Identifying non-resident clients may prove to be more difficult if they are not present and as such, could raise the inherent level of risk.
Your client has offshore business activities or interests	Is there a legitimate reason for your client to have offshore interests? 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	Take your client's connection to high-risk countries into account as some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or present a greater risk for crime, corruption or TF.

Table 11: Relationship-based examples of higher risk indicators and considerations for new developments and technologies

Examples of higher risk indicators	Considerations
Changing payment methods	The variety of payment methods made possible by advancements in technology is a potential risk for ML/TF. Many countries and companies have moved to a "cashless world" approach. As a result, clients are using alternative payment methods such as e-wallets. It is important to analyze the risk associated with these payment methods (for example, anonymity, borderless transactions, speed of the transactions, vulnerabilities in terms of know your client requirements) to determine how the technology used by your clients may increase their risk level.

A new service or activity that offers transaction anonymity	It is important to assess the impact that a new service or activity can have on the behaviour of your clients who may use it to distance themselves from a transaction.

Table 12: Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity

Examples of higher 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 you file a terrorist property report, the client automatically becomes high-risk.
Your client is a foreign PEP	A foreign PEP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence they may hold, a foreign PEP, their family members and their close associates are vulnerable to ML/TF and other offences such as corruption. As a business, you **must** consider a foreign PEP, their family members and their close associates as a high-risk client.
The entity has a complex structure that conceals the identity of beneficial owners	When you cannot obtain or confirm the ownership and control information of a corporation or an entity, you are required to verify the identity of the most senior managing officer of the entity and treat the entity as high-risk, and apply the prescribed special measures as stated in the Proceeds of Crime Money Laundering and Terrorist Financing Regulations. For more information, please consult FINTRAC's Beneficial ownership requirements guidance. It is important to note that when you do have the information on beneficial ownership, there may be other information or indicators that would make this relationship pose a higher risk.

Table 13: Relationship-based examples of additional higher risk indicators and related considerations

Examples of higher risk indicators	Considerations
STR was previously filed or considered	Suspicious transactions (or attempted transactions) are financial transactions for which you have reasonable grounds to suspect they are related to the commission or attempted commission of an **ML/TF offence**. For more information about STRs and ML/TF indicators, see FINTRAC's STR guidance. Clients that are the conductors of suspicious transactions that have been reported should be assessed as posing a higher risk.
Transactions involving third parties	Transactions involving third parties may indicate high-risk when the link between the third party and the client is not obvious.
The account activity does not match the client profile	Account activity that does not match the client profile may indicate a higher risk of ML/TF. You may face situations where you have submitted several large cash transaction reports to FINTRAC about a client with an occupation that does not match this type of activity (for example, 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 (such as a bar, a club, etc.)	Certain types of business, especially those that are cash-intensive may have a higher inherent risk for ML/TF because legitimate money can be co-mingled with illegitimate money. For 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 ML activity. Additionally, the 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 make the online gambling industry inherently higher risk. As well, 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 transactions) seems unusually or unnecessarily complex	An unnecessarily complex business structure or complex client transactions (compared to what you normally see in a similar circumstance) may indicate that the client is trying to hide transactions or suspicious activities.
Your client is a financial institution with which you have a correspondent banking relationship; **or** Your client is a correspondent bank that has been subject to sanctions.	Some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or simply present a greater risk for crime, corruption or TF. Additionally, the nature of the businesses that your correspondent bank client engages in and the type of markets it serves may present greater risks. The fact that your client has been subject to sanctions should raise the risk level and you should put appropriate measures in place to monitor the account.
Your client is an RE under the 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 can also increase the overall risks of ML/TF.

Your client is an intermediary or a gatekeeper (such as a lawyer or accountant) holding accounts for others unknown to you	Accountants, lawyers and other professionals sometimes hold co-mingled funds accounts for which beneficial ownership may be difficult to verify. This does not mean that all clients with these occupations are high-risk. You need to be aware of the risks that exist for these occupations and determine if the activities of the clients are in line with what you would expect and with the intended purpose of the account (for example a personal, business or trust account).
Your client is an unregistered charity	Individuals and organizations can misuse charities in ML schemes or to finance or support terrorist activity. It is important to be aware of the risks in relation to charities and to apply due diligence by confirming if a charity is registered with the Canada Revenue Agency
Domestic PEPs and heads of international organizations (HIOs)	Corruption is the misuse of public power for private benefit. Internationally, as well as in Canada, it is important to understand that the possibility for corruption exists and that domestic PEPs or HIOs can be vulnerable to carrying out or being used for ML/TF offences. Once you have determined that a person is a domestic PEP, a HIO or a family member or close associate of them, you must determine if the person poses a higher risk for committing an ML/TF offence. If you assess the risk to be high, then you must treat the person as a high-risk client. For more information, please consult the PEP and HIO guidance for your sector (if applicable).

1 Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 156(1)(c) (as will be amended when SOR/2019-240 comes into force) and Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c 17, s. 9.6(2).

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

3 PCMLTFR, SOR/2002-184, s. 156(1)(c)(ii) (as will be amended when SOR/2020-112 comes into force).

4 PCMLTFR, SOR/2002-184, s. 156(1)(c)(iii) (as will be amended when SOR/2019-240 comes into force).

5 PCMLTFR, SOR/2002-184, s. 156(2) (as will be amended when SOR/2020-112 comes into force).

6 PCMLTFR, SOR/2002-184, s. 156(1)(c)(i) (as will be amended when SOR/2019-240 comes into force).

7 PCMLTFR, SOR/2002-184, s. 156(1)(c)(iv) (as will be amended when SOR/2019-240 comes into force).

8 PCMLTFR, SOR/2002-184, s. 156(1)(c)(v) (as will be amended when SOR/2019-240 comes into force).

9 PCMLTFR, SOR/2002-184, s. 123.1(b) (as will be amended when SOR/2020-112 comes into force).

10 PCMLTFR, SOR/2002-184, s. 123.1(c) (as will be amended when SOR/2020-112 comes into force).

11 PCMLTFR, SOR/2002-184, s. 157 (as will be amended when SOR/2020-112 comes into force) and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).

12 Ibid.

13 Ibid.

14 PCMLTFR, SOR/2002-184, s. 145 (as will be amended when SOR/2019-240 comes into force).

15 PCMLTFR, SOR/2002-184, s. 123.1 (as will be amended when SOR/2020-112 comes into force).

16 PCMLTFR, SOR/2002-184, s. 157 (as will be amended when SOR/2020-112 comes into force) and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).

17 Ibid.

18 PCMLTFR, SOR/2002-184, ss. 123.1 (as will be amended when SOR/2020-112 comes into force) and 146(1) (as will be amended when SOR/2019-240 comes into force).

19 PCMLTFR, SOR/2002-184, s. 157 (as will be amended when SOR/2020-112 comes into force) and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).

20 PCMLTFR, SOR/2002-184, ss. 156(1)(c) and 156(2) (as will be amended when SOR/2020-112 comes into force) and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).

21 PCMLTFR, SOR/2002-184, ss. 156(3) and 156(1)(f) (as will be amended when SOR/2019-240 comes into force).

22 PCMLTFR, SOR/2002-184, s. 123.1(b) (as will be amended when SOR/2020-112 comes into force).

23 PCMLTFR, SOR/2002-184, ss. 123.1 and 157(b)(ii) (as will be amended when SOR/2020-112 comes into force).

24 PCMLTFR, SOR/2002-184, s. 123.1(b) (as will be amended when SOR/2020-112 comes into force).

25 PCMLTFR, SOR/2002-184, s. 123.1 (as will be amended when SOR/2020-112 comes into force).

26 PCMLTFR, SOR/2002-184, s. 157(b)(ii) (as will be amended when SOR/2020-112 comes into force).

27 PCMLTFR, SOR/2002-184, ss. 156(1)(f) and 156(3) (as will be amended when SOR/2019-240 comes into force).

28 PCMLTFR, SOR/2002-184, s. 156(3) (as will be amended when SOR/2019-240 comes into force).

29 PCMLTFR, SOR/2002-184, s. 156(4) (as will be amended when SOR/2019-240 comes into force).

Ibid.