FINTRAC — Canada FIU

Risk assessment guidance

Overview

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. You are responsible for completing and documenting your own risk assessment. However, FINTRAC does not prescribe how a risk assessment should be conducted. Rather, this guidance explains an internationally recognized way of conducting a risk assessment using an RBA and provides you with other tools that may help you meet your risk assessment obligations. For more information about your risk assessment obligations see FINTRAC's Compliance program requirement guidance

Who is this guidance for

- All reporting entities (REs)

In this guidance

1. What is the 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

Related guidance

- Compliance program requirements guidance.

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. 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 relationship 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 assessmen** of your business activities and clients taking into consideration certain elements, including:
    - your products, services and delivery channels;
    - the geographic location of your activities;
    - new developments and technologies;
    - your clients and business relationships;
    - the activities of your foreign and domestic affiliates — 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.
- **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; reassessing the level of risk associated with transactions and activities; and
    - applying **enhanced or special measures** to those transactions and business relationships identified as high-risk.
- 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.

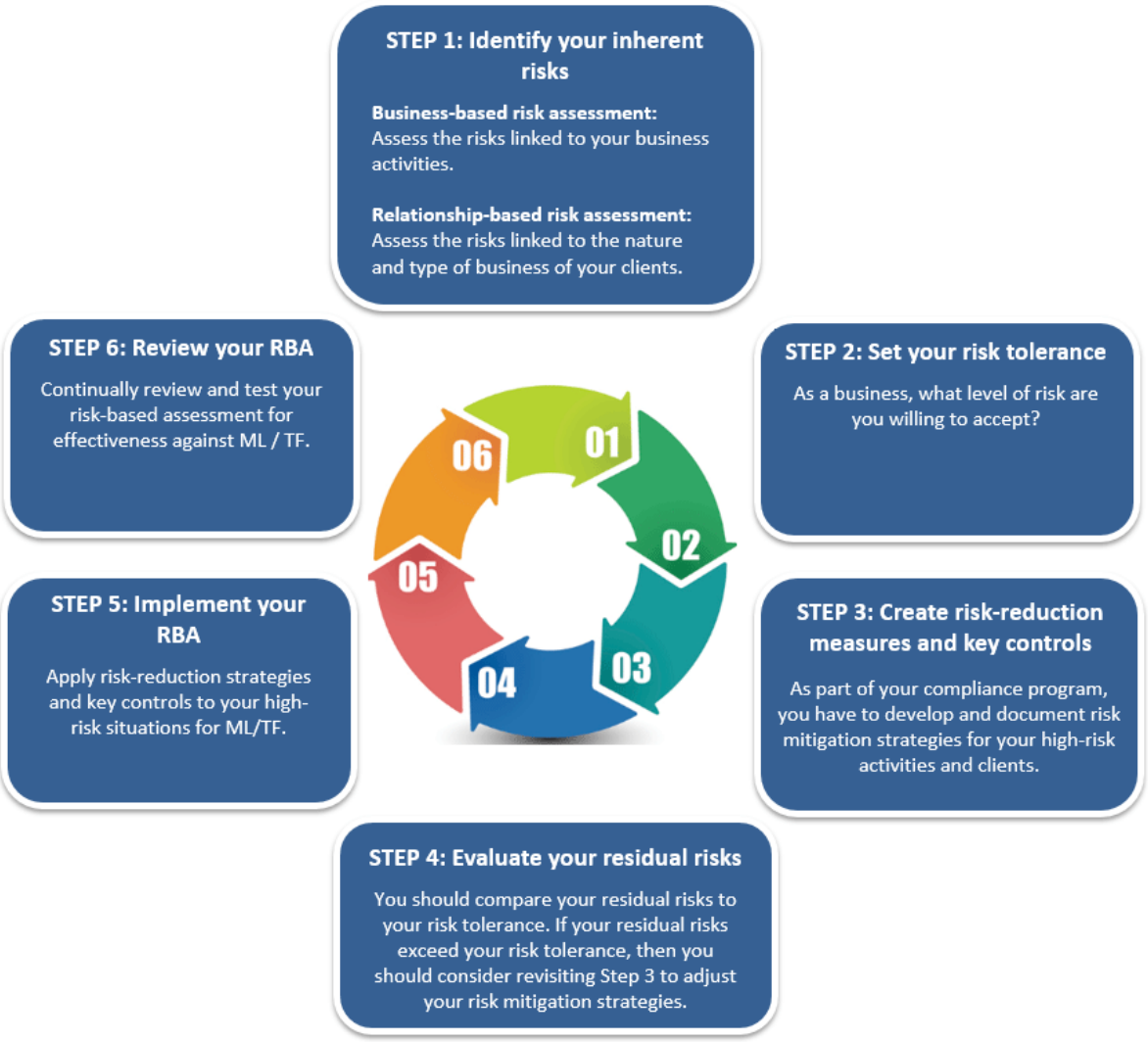
It is important to remember that assessing and mitigating the risk of ML/TF is not a static exercise. The risks you identify may change or evolve over time as new products, services, affiliations, or developments and technologies enter your business or its environment. You should be regularly reassessing 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 below.

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. 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 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. 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 crossing.	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. 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. 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.
- 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.

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.
3. **For all your clients and business relationships**, you will be required to:
    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:
    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. 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:

- 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.