

## **Guideline 4: Implementation of a Compliance Regime**

**Table of Contents**  
December 2008

This replaces the previous version of *Guideline 4: Implementation of a Compliance Regime* issued in February 2008. The changes made are indicated by a side bar to the right of the modified text.

<b>1</b>	<b>General .....</b>	<b>4</b>
<b>2</b>	<b>Who Has to Implement a Compliance Regime? .....</b>	<b>5</b>
2.1	Financial Entities .....	5
2.2	Life Insurance Companies, Brokers and Independent Agents .....	6
2.3	Securities Dealers .....	6
2.4	Casinos.....	7
2.5	Real Estate Brokers or Sales Representatives.....	7
2.6	Agents of the Crown that Sell or Redeem Money Orders .....	8
2.7	Money Services Businesses.....	8
2.8	Accountants and Accounting Firms .....	9
2.9	Dealers in Precious Metals and Stones .....	9
2.10	British Columbia Notaries .....	10
<b>3</b>	<b>What is a Compliance Regime?.....</b>	<b>10</b>
<b>4</b>	<b>Appointment of a Compliance Officer.....</b>	<b>11</b>
<b>5</b>	<b>Compliance Policies and Procedures .....</b>	<b>12</b>
<b>6</b>	<b>Risk-Based Approach.....</b>	<b>13</b>
6.1	Risk assessment .....	14
6.2	Risk mitigation .....	18
6.3	Keeping client identification and beneficial ownership information .....	
	up to date.....	21
6.4	Ongoing monitoring .....	22
6.5	High risk situations for certain sectors .....	23
<b>7</b>	<b>Ongoing Compliance Training.....</b>	<b>24</b>
<b>8</b>	<b>Review Every Two Years.....</b>	<b>26</b>
<b>9</b>	<b>FINTRAC's Approach to Compliance Monitoring .....</b>	<b>28</b>
<b>10</b>	<b>Penalties for Non-Compliance.....</b>	<b>29</b>
<b>11</b>	<b>Comments? .....</b>	<b>29</b>

<b>12 How to Contact FINTRAC.....</b>	<b>30</b>
<b>Appendix 1: Products, Services, Delivery Channels and Geographic Locations.....</b>	<b>31</b>
<b>Appendix 2: Client and Business Relationships.....</b>	<b>34</b>
<b>Appendix 3: Risk Level Assessment Matrix .....</b>	<b>37</b>

# 1 General

The objective of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) is to help detect and deter money laundering and the financing of terrorist activities. It is also to facilitate investigations and prosecutions of money laundering and terrorist activity financing offences. This includes implementation of reporting, record keeping, client identification and compliance regime requirements for the persons or entities described in section 2.

If you are one of these persons or entities, this guideline has been prepared to help you implement your compliance regime to meet your reporting, record keeping and client identification obligations.

Information is included about new obligations or changes to existing obligations that took effect on June 23, 2008. If you need information about requirements in effect before June 23, 2008, consult the previous version of this guideline (November 2003).

This guideline uses plain language to explain the most common situations under the Act as well as the related Regulations. It is provided as general information only. It is not legal advice, and is not intended to replace the Act and Regulations.

For more information about money laundering, terrorist financing or other requirements under the Act and Regulations, see the guidelines in this series:

- *Guideline 1: Backgrounder* explains money laundering and terrorist financing and their international nature. It also provides an outline of the legislative requirements as well as an overview of FINTRAC's mandate and responsibilities.
- *Guideline 2: Suspicious Transactions* explains how to report a suspicious transaction. It also provides guidance on how to identify a suspicious transaction, including general and industry-specific indicators that may help when conducting or evaluating transactions.
- *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* explains when and how to submit suspicious transaction reports. There are two different versions of Guideline 3, by reporting method.
- *Guideline 4: Implementation of a Compliance Regime* explains the requirement for reporting persons and entities to implement a regime to ensure compliance with their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated Regulations.
- *Guideline 5: Submitting Terrorist Property Reports to FINTRAC* explains when and how to submit a terrorist property report.
- *Guideline 6: Record Keeping and Client Identification* explains the requirement for reporting persons and entities to identify their clients and

keep records. There are several different versions of Guideline 6, with each one applicable to a particular sector.

- *Guideline 7: Submitting Large Cash Transaction Reports to FINTRAC* explains when and how to submit large cash transaction reports. There are two different versions of Guideline 7, by reporting method.
- *Guideline 8: Submitting Electronic Funds Transfer Reports to FINTRAC* explains when and how to submit electronic funds transfer reports. There are three different versions of Guideline 8, by report type and reporting method.
- *Guideline 9: Submitting Alternative to Large Cash Transaction Reports to FINTRAC* explains when and how financial entities can choose the alternative to large cash transaction reports. This is only applicable to financial entities.

If you need more help after you read this or other guidelines, call FINTRAC's national toll-free enquiries line at 1-866-346-8722.

Your compliance policies and procedures may cover situations other than the ones described in this guideline, for purposes other than your requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. For example, the federal or provincial regulator for your sector may require you to apply additional compliance policies and procedures other than what is described in this guideline.

## **2 Who Has to Implement a Compliance Regime?**

### **2.1 Financial Entities**

If you are a financial entity, such as a bank, credit union, caisse populaire, trust company, loan company or an agent of the Crown that accepts deposit liabilities, you have to implement a compliance regime to comply with your reporting, record keeping and client identification requirements.

#### **Foreign subsidiaries or foreign branches**

Effective June 23, 2008, if your financial entity has foreign subsidiaries or foreign branches that are located in a country that is not a member of the Financial Action Task Force and that carry out activities similar to yours or to a life insurance company or securities dealer, you have to ensure that they develop and apply policies and procedures consistent with your compliance regime requirements here in Canada. If the laws of the country in which your subsidiary operates prohibit compliance with these requirements, you have to keep a record to that effect. See *Guideline 6G: Record Keeping and Client Identification for Financial Entities* for more information.

## 2.2 Life Insurance Companies, Brokers and Independent Agents

If you are a life insurance company, broker or independent agent, you have to implement a compliance regime to comply with your reporting, record keeping and client identification requirements.

If you are an employee of a person or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, when life insurance agents are employees of a life insurance company, the compliance regime requirement is the responsibility of the life insurance company. If you are a life insurance broker or independent agent (i.e., you are not an employee), you are responsible for your own compliance regime.

### **Foreign subsidiaries or foreign branches**

Effective June 23, 2008, if your life insurance company has foreign subsidiaries or foreign branches that are located in a country that is not a member of the Financial Action Task Force and that carry out activities similar to yours or to a financial entity or securities dealer, you have to ensure that they develop and apply policies and procedures consistent with your compliance regime requirements here in Canada. If the laws of the country in which your subsidiary operates prohibit compliance with these requirements, you have to keep a record to that effect. See *Guideline 6A: Record Keeping and Client Identification for Life Insurance Companies, Brokers and Agents* for more information.

## 2.3 Securities Dealers

If you are **provincially authorized** to engage in the business of dealing in securities or any other financial instruments, portfolio management or investment advising services, you have to implement a compliance regime to comply with your reporting, record keeping and client identification requirements.

If you are an employee of a person or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, if you are an employee of an entity engaged in the business of dealing in securities, the compliance regime requirement is the responsibility of the entity.

Similarly, if you are an agent of (or you are authorized to act on behalf of) a person or entity who is also subject to these requirements, that other person or entity is responsible for the compliance regime.

### **Foreign subsidiaries or foreign branches**

Effective June 23, 2008, if your securities dealer is an entity that has foreign subsidiaries or foreign branches that are located in a country that is not a member of the Financial Action Task Force and that carry out activities similar to yours or to a financial entity or life insurance company, you have to ensure that they develop and apply policies and procedures consistent with your compliance

regime requirements here in Canada. If the laws of the country in which your subsidiary operates prohibit compliance with these requirements, you have to keep a record to that effect. See *Guideline 6E: Record Keeping and Client Identification for Securities Dealers* for more information.

## 2.4 Casinos

If you are a casino authorized to do business in Canada, you have to implement a compliance regime if roulette or card games are carried on in your establishment, or if your establishment has a slot machine. In this context, a slot machine does not include a video lottery terminal.

If you are a registered charity, you may be authorized to do business only temporarily as a casino for charitable purposes. If this is your situation and you carry on business in the casino for two consecutive days or less under the supervision of the casino, you do not have to implement a compliance regime. If you are the supervising casino (i.e., the permanent establishment in which a charity casino operates), you remain responsible for the compliance regime, as well as the reporting and record keeping requirements under the Act and Regulations.

## 2.5 Real Estate

### **Real estate brokers or sales representatives**

If you are a real estate broker or sales representative, you have to implement a compliance regime when you act as an agent in the purchase or sale of real estate. However, these requirements do not apply to you for activities related to property management.

If you are an employee of a person or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, if you are a sales representative who is an employee of a real estate broker, the compliance regime requirement is the responsibility of the broker.

### **Real estate developers**

A real estate developer means an individual or an entity other than a real estate broker or sales representative, who in any calendar year after 2007 has sold one of the following to the public:

- at least five new houses or condominium units;
- at least one new commercial or industrial building;
- at least one new multi-unit residential building each of which contains five or more residential units; or
- at least two new multi-unit residential buildings that together contain five or more residential units.

Effective February 20, 2009, if you are a real estate developer, you have to implement a compliance regime if you sell any of the following to the public:

- a new house;
- a new condominium unit;
- a new commercial or industrial building; or
- a new multi-unit residential building.

If you are an entity that is a corporation, you are subject to this whether you sell those buildings on your own behalf or on behalf of a subsidiary or affiliate. In this context, an entity is affiliated with another entity if one of them is wholly-owned by the other or both are wholly-owned by the same entity.

## **2.6 Agents of the Crown that Sell or Redeem Money Orders**

If you are a government department or an agent of the Crown (i.e., an agent of her Majesty in right of Canada or of a province), you have to implement a compliance regime if you sell or redeem money orders.

If you accept deposit liabilities in the course of providing financial services to the public, such as a provincial savings office, you are considered a financial entity (see subsection 2.1).

If you are an agent of the Crown that sells precious metals to the public, you are considered a dealer in precious metals and stones (see subsection 2.9).

## **2.7 Money Services Businesses**

Effective June 23, 2008, a money services business will include foreign exchange dealers. Therefore, you are a money services business if you are a person or entity engaged in the following business activities:

- foreign exchange dealing;
- remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network; or
- issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments.

This includes alternative money remittance systems, such as Hawala, Hundi, Chitti, etc.

If you are a money services business, you have to implement a compliance regime to comply with your reporting, record keeping and client identification requirements when you engage in any of the business activities described above. This does not include redeeming cheques payable to a named person or entity. In other words, if you are only involved in cashing cheques made out to a particular person or entity, you are not subject to this requirement.

If you are an employee of a money services business, it is your employer who is engaged in the business and therefore responsible for the compliance regime. If you are an agent of (or you are authorized to act on behalf of) another person or entity that is a money services business, that other person or entity is responsible for the compliance regime for the relevant activities that you perform on their behalf.

## **2.8 Accountants and Accounting Firms**

If you are an accountant or an accounting firm, you have to implement a compliance regime if you engage in any of the following activities on behalf of any person or entity (other than your employer) or give instructions in respect of those activities on behalf of any person or entity (other than your employer):

- receiving or paying funds;
- purchasing or selling securities, real property or business assets or entities; or
- transferring funds or securities by any means.

You are subject to this whether or not you receive professional fees for these activities. However, effective June 23, 2008, you are not subject to this regarding the professional fees themselves.

The activities listed above do not include audit, review or compilation work carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook.

If you are an employee of a person or entity who is also subject to these requirements, your employer is responsible for the compliance regime. For example, if you are an accountant who is an employee of an accounting firm, the compliance regime requirement is the responsibility of the firm.

Similarly, if you are an agent of (or you are authorized to act on behalf of) a person or entity who is also subject to these requirements, that other person or entity is responsible for the compliance regime.

## **2.9 Dealers in Precious Metals and Stones**

A dealer in precious metals and stones (DPMS) means an individual or an entity that buys or sells precious metals, precious stones or jewellery, in the course of its business activities. Precious metals include gold, silver, palladium or platinum whether in coins, bars, ingots, granules or in any other similar form. Precious stones include diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. Jewellery means objects made of precious metals, precious stones or pearls intended for personal adornment.

If you are a DPMS, effective December 30, 2008, you have to implement a compliance regime if you engage in the purchase or sale of precious metals, precious stones or jewellery in an amount of \$10,000 or more in a single transaction. However, you are not subject to this if you engage only in purchases or sales carried out for, in connection with, or for the purpose of manufacturing jewellery, extracting precious metals or precious stones from a mine or cutting or polishing precious stones.

An agent of the Crown (i.e., a government department or an agent of her Majesty in right of Canada or of a province) is considered to be a DPMS effective December 30, 2008, when it sells precious metals to the public in an amount of \$10,000 or more in a single transaction.

## **2.10 British Columbia Notaries**

A British Columbia notary means a British Columbia notary public or a British Columbia notary corporation. In this context, a notary public means an individual who is a member of the Society of Notaries Public of British Columbia. Also in this context, a notary corporation means an entity that provides notary services to the public in British Columbia under the *Notaries Act* of that province.

If you are a British Columbia notary, effective December 30, 2008, you have to implement a compliance regime if you engage in any of the following activities on behalf of any individual or entity (other than your employer), or give instructions on behalf of any individual or entity (other than your employer):

- receiving or paying funds (other than those received or paid for professional fees, disbursements, expenses or bail);
- purchasing or selling securities, real property or business assets or entities; or
- transferring funds or securities by any means.

## **3 What is a Compliance Regime?**

The implementation of a compliance regime is good business practice for anyone subject to the Act and its Regulations. A well-designed, applied and monitored regime will provide a solid foundation for compliance with the legislation. As not all persons and entities operate under the same circumstances, your compliance regime will have to be tailored to fit your individual needs. It should reflect the nature, size and complexity of your operations.

If you are a member of an association within your sector of activity, you may wish to check with them to find out if any information sharing about any aspect of compliance regime implementation is available. You may also check with any regulatory body covering your sector in this regard.

Your compliance regime has to include the following:

- the appointment of a compliance officer (see section 4);
- the development and application of compliance policies and procedures. Effective June 23, 2008, these policies and procedures have to be written and kept up to date. If you are an entity, they also have to be approved by a senior officer (see section 5);
- effective June 23, 2008, an assessment and documentation of risks related to money laundering and terrorist financing (see section 6);
- if you have employees or agents or any other individuals authorized to act on your behalf, an on-going compliance training program for them. Effective June 23, 2008, the training program has to be in writing and maintained (see section 7); and
- a review of your compliance policies and procedures to test their effectiveness. Effective June 23, 2008, the review has to cover your policies and procedures, your assessment of risks related to money laundering and terrorist financing and your training program. The review also has to be done every two years (see section 8).

These five elements are key to any effective system of internal controls and are expanded upon in sections 4 to 8.

## **4 Appointment of a Compliance Officer**

The individual you appoint will be responsible for the implementation of your compliance regime. Your compliance officer should have the authority and the resources necessary to discharge his or her responsibilities effectively. Depending on your type of business, your compliance officer should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

If you are a small business, the appointed officer could be a senior manager or the owner or operator of the business. If you are an individual, you can appoint yourself as compliance officer or you may choose to appoint another individual to help you implement a compliance regime.

In the case of a large business, the compliance officer should be from a senior level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed compliance officer in a

large business should not be directly involved in the receipt, transfer or payment of funds.

For consistency and ongoing attention to the compliance regime, your appointed compliance officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the compliance officer retains responsibility for the implementation of the compliance regime.

## **5 Compliance Policies and Procedures**

An effective compliance regime includes policies and procedures and shows your commitment to prevent, detect and address non-compliance. Effective June 23, 2008, your compliance program has to include written policies and procedures to assess the risks related to money laundering and terrorist financing in the course of your activities.

The level of detail of these policies and procedures depends on your needs and the complexity of your business. It will also depend on your risk of exposure to money laundering or terrorist financing. See section 6 for more information on risk-based approach.

For example, the compliance policies and procedures of a small business may be less detailed and simpler than those of a large bank. However, effective June 23, 2008, your policies and procedures have to be in writing and be kept up to date, whether you are a small business, an individual or an entity. Several factors could trigger the need to update, as often as necessary, your policies and procedures, such as changes in legislation, non-compliance issues, or new services or products.

In addition, if you are an entity, your policies and procedures also have to be approved by a senior officer. A senior officer of an entity includes its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any person who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

It is important that your compliance policies and procedures are communicated, understood and adhered to by all within your business who deal with clients or any property owned or controlled on behalf of clients. This includes those who work in the areas relating to client identification, record keeping, and any of the types of transactions that have to be reported to FINTRAC. They need enough

information to process and complete a transaction properly as well to identify clients and keep records as required.

They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering or anti-terrorist financing regimes consistent with international standards. See additional information about this in subsection 6.1.2 and Appendix 1.

Your compliance policies and procedures should incorporate, at a minimum, the reporting, record keeping, client identification, risk assessment and risk-mitigation requirements applicable to you. For example, in the case of your reporting obligations relating to terrorist property or suspicions of terrorist financing, your policies and procedures should include the verification of related lists published in Canada. These are available on the Office of the Superintendent of Financial Institutions' Web site at <http://www.osfi-bsif.gc.ca>, by referring to the "Terrorism Financing" link.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

## **6 Risk-Based Approach**

Effective June 23, 2008, your compliance regime has to include an assessment and documentation of risks related to money laundering and terrorist financing in a manner that is appropriate to you. This is in addition to your client identification, record keeping and reporting requirements. A risk-based approach is a process that allows you to identify potential high risks of money laundering and terrorist financing and develop strategies to mitigate them. Existing obligations, such as your client identification will be maintained as a minimum baseline requirement. However, when it comes to situations where enhanced due diligence is appropriate, a principle of risk-based approach is to focus your resources where they are most needed to manage risks within your tolerance level. You have to determine what is acceptable for you, taking into account the nature of each product or service, the geographical regions where you do your business and the relationships you have with your clients.

The approach to the management of risk and risk-mitigation requires the leadership and engagement of senior management towards the detection and deterrence of money laundering and terrorist financing. Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of money laundering and terrorist financing within a business.

## What is a risk-based approach?

In the context of money laundering and terrorist financing, a risk-based approach is a process that encompasses the following:

- the **risk assessment** of your business activities using certain factors;
- the **risk mitigation** to implement controls to handle identified risks;
- keeping **client identification** and, if required for your sector, **beneficial ownership information** up to date; and
- the **ongoing monitoring** of financial transactions that pose higher risks.

These, as well as additional requirements for certain sectors, are explained in further detail in subsections 6.1 to 6.5.

## 6.1 Risk assessment

A risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which your business is exposed. The complexity of the assessment depends on the size and risk factors of your business.

While performing your risk assessment, you should refer to *Guideline 1: Backgrounder* for additional information on money laundering and terrorist financing and *Guideline 2: Suspicious Transactions* for additional common and industry-specific indicators related to your products and services as well as to occupation, business, financial history and past transaction patterns of your clients. These may help you in completing your risk assessment. Industry associations or regulators may also provide guidance that can be of assistance to you in this area.

You have to document and consider the following factors in your assessment:

- your products and services and the delivery channels through which you offer them;
- the geographic locations where you conduct your activities and the geographic locations of your clients;
- other relevant factors related to your business; and
- your clients and the business relationships you have with them.

You may want to perform the risk assessment for your business in two stages:

- Stage 1: Business-based risk assessment of your products, services, delivery channels and the geographic location in which your business operates.
- Stage 2: Relationships-based risk assessment of products and services your clients utilize as well as the geographic locations in which they operate or do business.

To help you assess products, services, delivery channels and geographic locations that may pose higher risks of money laundering or terrorist financing,

we have developed a list of questions in a checklist format (see Appendix 1) as well as a risk matrix (see Appendix 3).

Similarly, for clients and ongoing business relationships that may pose higher risks of money laundering or terrorist financing, we have developed a list of the most common risk categories in a checklist format (see Appendix 2). See also subsection 6.1.4 for more information.

Checklists in Appendices 1 and 2 provide examples to facilitate the assessment of the above factors. However, your risk assessment has to be appropriate for your specific business needs which means that it may have to be more detailed than the checklists provided. You can customize the checklists or you can use a different method or another tool. For example, this could take the form of establishing clusters of clients with different risk variables (e.g. products used, geographic location, transaction volumes, business industries engaged in, duration of the relationship, or other factors identified by your business). You could then give the separate clusters a weighting commensurate with the risk of potential money laundering and terrorist financing.

Your risk assessment may identify high risk situations for which risk-mitigation controls and monitoring may be required. See subsections 6.2 and 6.4 for more information.

Risk assessment requires good knowledge of your business operations and sound judgment exercised by your personnel so the risks for money laundering and terrorist financing can be weighed according to each individual factor as well as a combination of them. Your risk assessment is not static and will change over time.

If you are a financial entity or a securities dealer, you have additional requirements related to risk assessment. See subsection 6.5 for more information.

### **6.1.1 Products, services and delivery channels**

You have to be aware of and recognize products and services or combinations of them that may pose higher risks of money laundering or terrorist financing. Legitimate products and services can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. For example, these could include a money laundering related sale of high value goods that resulted in a cheque payable to a bearer which is then deposited into another individual's account to make the transaction difficult to trace and detect.

In addition, you may also consider services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering or terrorist financing. For example, international correspondent banking services, international private banking services, or services involving banknote and precious metal trading and delivery.

You have to consider, in a manner that is appropriate to you, the channels used to deliver your products or services. In today's economy and global market, many delivery channels do not bring the client into direct face-to-face contact with you (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The more remote a client is from you, the more likely you will have to depend on a third party to deliver your products or services. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks.

In addition, you should consider new or innovative services or delivery channels that you may use to deliver your products or services.

### **6.1.2 Geographic locations**

You have to consider, in a manner that is appropriate to you, whether geographic locations in which you operate or undertake activities pose a potentially higher risk for money laundering and terrorist financing. Depending on your business and operations, geographic locations can range from your immediate surroundings, whether rural or urban to a province or territory, multiple jurisdictions within Canada (domestic) or other countries.

For example, large entities that operate in a number of domestic jurisdictions may refine the geographic locations factor to differentiate between urban locations having known higher crime rates in comparison to other urban or rural districts. Smaller entities that restrict their activities to a single geographic location or district may not need to make that distinction.

### **6.1.3 Other relevant factors**

You need to consider, in a manner that is appropriate to you, any other factors that are relevant to you, your business or sector. For example, you may offer products or services that can be used to convert funds to a more liquid form, such as electronic wallet, internet payment services or mobile payments. Your business activities may also be more attractive to launder money or fund terrorist activity.

*Guideline 1: Backgrounder* and *Guideline 2: Suspicious Transactions* have more information about money laundering and terrorist financing that can help you in your risk assessment. You should also periodically review whether additional

factors have become relevant to your situation, like risks arising from innovative or emerging technologies.

#### **6.1.4 Clients and business relationships**

The guidance below does not prohibit you from engaging in transactions with potential clients but provides you with information to effectively manage potential money laundering and terrorist financing risks.

You have to consider the nature and business of your clients and their relationships with you to determine the level of risk of money laundering and terrorist financing. In other words, you have to know your clients to perform a risk assessment. Knowing your clients is not limited to identification or record keeping requirements. It is about understanding your clients, including their activities, transaction patterns, how they operate and so on. Other elements, such as the magnitude of a client's assets or the number of transactions involved, might also be relevant. Although you should obtain this information through your dealings with the client, it does not necessarily mean that you have to ask the client for additional information or identification documents. You should consider clients you do not know as higher risk than those that you know.

Completing a client risk assessment should be appropriate where there is an ongoing relationship. An ongoing relationship is where a client opens an account or undertakes multiple transactions over a time period with you, regardless of whether the transactions are related to each other. Where your dealings with a client are limited to a single transaction, this is **not** considered to be an ongoing relationship. For example, a money services business would not have to perform a risk assessment for an individual client who conducts a single foreign exchange transaction to buy \$500 US dollars with Canadian dollars because it is not an ongoing relationship. However, if the transaction seems suspicious, the money services business has to report it to FINTRAC as explained in *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC*.

In addition to assessing risk regarding existing clients, for new clients, it is recommended that you perform a risk assessment at the beginning of a client relationship, although a comprehensive risk profile may only become evident once the client has conducted financial transactions with you. However, if you decide to complete a risk rating of new clients, the client identification and information gathering measures at account opening should be robust enough to provide the information needed to feed into your client risk assessment.

When assessing a client relationship, consider its duration, the client's number of accounts (if applicable), the products and services used and the client's activities. You may also consider third parties that can be involved in the client's relationship for their impact on the client's risk if you are required to make third party determination. Furthermore, you also have to consider the beneficial

owners of an entity for their impact on risk if you are required to obtain this information. See Guideline 6 for your sector for more information about third party determinations and beneficial ownership information requirements.

Situations where you facilitate a transaction for which a client is acting on behalf of a third party but does not know anything about the third party, may lead you to consider that client as a higher risk. Similarly, a client acting on behalf of an entity who is not aware of the entity's beneficial owners (such as the names of the entity's directors or the individuals controlling the entity for example), may lead you to consider that client as a higher risk.

If you know that your client is a politically exposed foreign person (even when you are not required to make the determination or keep related records), you should consider that client as being a higher risk. See the definition of a politically exposed foreign person in Appendix 2.

You should also consider unusual circumstances, cash-intensive businesses and other indicators as potential high risks.

## **6.2 Risk mitigation**

Risk mitigation is about implementing controls to limit the potential money laundering and terrorist financing risks you have identified while conducting your risk assessment to stay within your risk tolerance level. As part of your compliance program, when your risk assessment determines that risk is high for money laundering or terrorist financing, you have to develop written risk-mitigation strategies (policies and procedures designed to mitigate high risks) and apply them for high risks situations.

### **6.2.1 Measures to mitigate the risks**

You have to include risk-mitigation measures in your written policies and procedures. The following summarizes different types of mitigating measures you could develop and apply through your compliance policies and procedures.

#### **Effective internal controls**

You should consider internal controls such as:

- focussing on your operations (products, services, clients and geographic locations) that are more vulnerable to abuse by money launderers and criminals;
- informing senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious transaction reports filed;
- providing for program continuity despite changes in management, employees or structure;

- focussing on meeting all regulatory record keeping and reporting requirements, recommendations for anti-money laundering and anti-terrorist financing compliance and provide for timely updates in response to changes in requirements;
- enabling the timely identification of reportable transactions and ensure accurate filing of required reports;
- incorporating anti-money laundering and anti-terrorist financing compliance into job descriptions and performance evaluations of appropriate personnel; and
- providing for adequate supervision of employees that handle currency transactions, complete reports, monitor for suspicious transactions, or engage in any other activity that forms part of your anti-money laundering and anti-terrorist financing program.

## **Generic measures**

These may include the following:

- increase your awareness of higher risk situations within business lines across your entity;
- increase the monitoring of transactions;
- escalate the approval of the establishment of an account or relationship even if you are not otherwise required to do so (see additional requirements for certain sectors in subsection 6.5);
- increase the levels of ongoing controls and reviews of relationships; and
- review your own internal controls, to ensure that you have:
  - personnel that have clear lines of authority, responsibility and accountability;
  - adequate segregation of duties (for example, an employee opening an account for a client is not authorized to also approve its opening as that authorization is the responsibility of someone else in the organization);
  - proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold has to follow a procedure to get approval for the transaction by someone else in the organization); and
  - internal reviews to validate the risk assessment processes.

## **Risk-focused measures**

You may consider additional measures such as:

- seeking additional information beyond the minimum requirements to substantiate the client's identity or the beneficial ownership of an entity;
- obtaining additional information about the intended nature of the relationship, including estimates regarding the amount and type of business activity;
- obtaining additional documented information regarding the client's source of funds and accumulation of wealth;
- requesting high risk clients to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
- getting independent verification of information (i.e. from a credible source other than the client);
- stopping any transaction with a potential client until identification and account opening information has been obtained;
- implementing an appropriate process to approve all relationships identified as high risk as part of the client acceptance process or declining to do business with potential clients because they exceed your risk tolerance level;
- implementing a process to exit from an existing high risk relationship which management sees as exceeding your risk tolerance level;

- analysing money laundering and terrorist financing risk vulnerabilities for your new acquisition processes and for product or service development processes.

If you are a financial entity, a securities dealer, a life insurance company, broker or independent agent, or a money services business, you have additional requirements related to risk mitigation. See subsection 6.5 for more information.

### **6.3 Keeping client identification and beneficial ownership information up to date**

When your risk assessment determines that risk is high for money laundering or terrorist financing, you have to develop and apply policies and procedures to keep client identification information up to date. If you are a financial entity, a securities dealer, a life insurance company, broker or agent, or a money services business, this also applies for keeping beneficial ownership information up to date.

#### **Client identification information**

Client identification information depends on the information you have to confirm or obtain from your clients and the records you have to keep. Client identification information that is required to be updated generally includes:

- For an **individual**, the individual's name, address, telephone number and occupation or principal business.
- For a **corporation**, its name and address and the names of the corporation's directors.
- For an **entity other than a corporation**, its name, address and principal place of business.

Reasonable measures to keep client identification up to date include asking the client to confirm or update their information. In the case of an individual client, reasonable measures also include confirming or updating the information through the options available to identify individuals who are not physically present. This can include obtaining information verbally to keep client identification information up to date.

In the case of clients that are entities, reasonable measures to keep client identification up to date include consulting a paper or an electronic document to confirm information or obtaining the information verbally from the client.

Although the frequency with which the client identification information is to be kept up to date will vary depending on your business, you should review it at least every two years for high risk situations. When you review client identification information, you should also update the records you keep for that client.

You may want to consider establishing and implementing a timeline to update the identification information of your clients that you do not consider high risk.

### **Beneficial ownership information**

If you are a financial entity, a securities dealer, a life insurance company, broker or independent agent, or a money services business, you have to take reasonable measures to obtain beneficial ownership information about entities in certain circumstances. Beneficial ownership information of an entity means the name, address and occupation of all the individuals that own or control, directly or not, 25% or more of the entity. If the entity is a corporation, beneficial ownership information also includes the name and occupation of all the corporation's directors. Guideline 6 for your sector has more information about beneficial ownership requirements. Reasonable measures to keep beneficial ownership up to date are the same as the ones explained for client identification information above. For high risk situations, the beneficial ownership should be updated at least every two years. When you review beneficial ownership information, you should also update the records you keep for that client.

## **6.4 Ongoing monitoring**

You have to take reasonable measures to conduct ongoing monitoring of financial transactions that pose high risks of money laundering and terrorist financing to detect suspicious transactions. Reasonable measures may involve manual or automated processes, or a combination of both depending on your resources and needs. They also depend on the size of your business and the risks to which you are exposed. You do not necessarily have to create or purchase an electronic system. You can use your available resources and business processes and build on these.

Your policies and procedures have to determine what kind of monitoring is done for particular high risk situations, including how to detect suspicious transactions. Your policies and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.

You could consider the following measures to monitor high risk situations:

- review transactions based on an approved schedule that involves management sign-off;
- develop reports or perform more frequent review of reports that list high risk transactions. Flag activities or changes in activities from your expectations and elevate concerns as necessary;
- set business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- review transactions more frequently against suspicious transaction indicators relevant to the relationship and escalate them should additional

indicators be detected. See *Guideline 2: Suspicious Transactions* for more information about indicators.

If you are a financial entity or a securities dealer, you have additional requirements related to ongoing monitoring of financial transactions. See subsection 6.5 for more information.

## **6.5 High risk situations for certain sectors**

In addition to the risk-based approach process described in subsections 6.1 to 6.4, certain sectors have further requirements. These are described below, by sector.

### **6.5.1 Financial entities**

#### **Ongoing monitoring for correspondent banking relationships**

Effective June 30, 2007, when you enter into a correspondent banking relationship with a foreign financial institution, you have to take reasonable measures to find out whether the foreign financial institution has anti-money laundering and anti-terrorist financing policies and procedures in place, including procedures for the approval of opening new accounts. In this context, reasonable measures include asking the foreign financial institution for the information about their policies and procedures. If it does not have such policies and procedures in place, you have to take reasonable measures to conduct ongoing monitoring of all transactions (as explained in subsection 6.4) within the correspondent banking relationship to detect suspicious transactions.

You could also consider monitoring transactions that you have flagged as questionable in the context of correspondent banking relationships such as the following:

- large value or large volume transactions that involve numbered monetary instruments (for example travellers' cheques, money orders or bank drafts);
- transactions that appear unusual in the context of the relationship; or
- transactions that appear to be structured to avoid your monitoring system.

In addition, you have to take reasonable measures to find out, based on publicly available information, whether there are any civil or criminal sanctions imposed against the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements. If there are any sanctions, the correspondent banking relationship is considered a higher risk. In that case, you have to take reasonable measures to conduct ongoing monitoring of all transactions within the correspondent banking relationship to detect suspicious transactions. To do so, consider the measures described above as well as those in subsection 6.4.

## **6.5.2 Financial entities and securities dealers**

### **Politically exposed foreign persons determination for existing and new account holders**

Effective June 23, 2008, if you are a financial entity or a securities dealer, your risk assessment must identify high risk situations for money laundering and terrorist financing where existing account holders (including credit card accounts opened by financial entities) might be politically exposed foreign persons. This means that your policies and procedures have to include reasonable measures to determine whether or not an existing account holder that is consider higher risk is a politically exposed foreign person. Effective June 23, 2008, you also have to take reasonable measures to determine whether or not a new account holder is a politically exposed foreign person. Whether for a new or an existing account, reasonable measures could include the automated review of your individual client base using commercial software or publicly available information about politically exposed foreign persons. You could also ask your clients.

Once you have determined that an account holder is a politically exposed foreign person, you have additional requirements. They include establishing the source of funds and getting senior management approval to keep an account open (whether for a new or an existing account). You also have to conduct enhanced ongoing monitoring of transactions related to the account to detect suspicious transactions. To do so, consider the measures described in subsection 6.4. See Guideline 6 for your sector for more information about politically exposed foreign persons.

## **6.5.3 Financial entities, life insurance companies, brokers or agents, or money services businesses**

### **Politically exposed foreign persons determination for certain transactions**

Effective June 23, 2008, if you are a financial entity, a life insurance company, broker or agent, or a money services business, you have additional requirements for certain types of transactions of \$100,000 or more. You have to determine if you are dealing with a politically exposed foreign person. If so, you have to establish the source of funds and get senior management to review the transaction. See Guideline 6 for your sector for more information about politically exposed foreign persons.

## **7 Ongoing Compliance Training**

If you have employees, agents or other individuals authorized to act on your behalf, your compliance regime has to include training. This is to make sure that all those who have contact with clients, who see client transaction activity, who handle cash or funds in any way or who are responsible for implementing or overseeing the compliance regime understand the reporting, client identification

and record keeping requirements. This includes those at the “front line” as well as senior management.

Effective June 23, 2008, your training program has to be in writing and you have to maintain it. This means that the program itself has to be in writing, but the way the training is delivered does not have to be in writing. For example, you could deliver your training program using computer-based software, information sessions, face-to-face meetings, etc. You also have to ensure that your training program is reviewed and adjusted in a timely manner to reflect your needs.

In addition, others who have responsibilities under your compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls, should receive training. This could also include the appointed compliance officer and internal auditors.

Standards for the frequency and method of training, such as formal, on-the-job or external, should be addressed. New people should be trained before they begin to deal with clients. All should be periodically informed of any changes in anti-money laundering or anti-terrorism legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs. Those who change jobs within your organization should be given training as necessary to be up-to-date with the policies, procedures and risks of exposure to money laundering or terrorist financing that are associated with their new job.

The method of training may vary greatly depending on the size of your business and the complexity of the subject matter. The training program for a small business may be less sophisticated.

When assessing your training needs, consider the following elements:

- **Requirements and related liabilities**

The training should give those who need it an understanding of the reporting, client identification and record keeping requirements as well as penalties for not meeting those requirements. For more information about this, see the other guidelines regarding each of those requirements applicable to you.

- **Policies and procedures**

The training should make your employees, agents, or others who act on your behalf aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs. It should also give each one a clear understanding of his or her responsibilities under these policies and procedures.

They need to understand how their institution, organization or profession is vulnerable to abuse by criminals laundering the proceeds of crime or by

terrorists financing their activities. Training should include examples of how your particular type of organization could be used to launder illicit funds or fund terrorist activity. This should help them to identify suspicious transactions and should give you some assurance that your services are not being abused for the purposes of money laundering or terrorist financing.

Employees should also be made aware that they cannot disclose that they have made a suspicious transaction report, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether it has started or not. They should also understand that no criminal or civil proceedings may be brought against them for making a report in good faith.

- **Background information on money laundering and terrorist financing**  
Any training program should include some background information on money laundering so everyone who needs to can understand what money laundering is, why criminals choose to launder money and how the process usually works. They also need to understand what terrorist financing is and how that process usually works. For more information about this, see *Guideline 1: Backgrounder* and FINTRAC's website (<http://www.fintrac-canafe.gc.ca>).

All businesses should consult, if possible, training material available through their associations. In addition, FINTRAC makes material available on its Web site that can provide help with training. For example, a practice environment is available within F2R, FINTRAC's Web-based tool for electronic reporting, that can be used for training. You can use this to complete simulated electronic reports. However, as a reporting person or entity described in section 2, you are responsible to have your own training program and to ensure that each component of the program is reviewed and adjusted to meet your needs.

## **8 Review Every Two Years**

Another component of a comprehensive compliance regime is a review of your compliance policies and procedures to test their effectiveness. Effective June 23, 2008, the review has to be done every two years. It has to cover your policies and procedures, your assessment of risks related to money laundering and terrorist financing and your training program to test their effectiveness. The review or your assessment of risks related to money laundering and terrorist financing has to cover all the components of the risk-based approach as explained in subsections 6.1 to 6.5, including risk assessment, risk-mitigation and ongoing monitoring. This will help evaluate the need to modify existing policies and procedures or to implement new ones. This may also lead you to update your compliance policies and procedures.

If you are in a sector that is regulated at the federal or provincial level, the need for review of your compliance policies and procedures could also be triggered by requirements administered by your regulator.

The review is to be conducted by an internal or external auditor, if you have one. The review by an internal or external auditor could include interviews, tests and samplings, such as the following:

- interviews with those handling transactions and with their supervisors to determine their knowledge of the legislative requirements and your policies and procedures.
- a review of the criteria and process for identifying and reporting suspicious transactions.
- a sampling of large cash transactions followed by a review of the reporting of such transactions.
- a sampling of international electronic funds transfers (if those are reportable by the reporting person or entity in question) followed by a review of the reporting of such transactions.
- a test of the validity and reasonableness of any exceptions to large cash transaction reports including the required annual report to FINTRAC (this is applicable only for financial entities who choose the alternative to large cash transactions for certain business clients).
- a test of the record keeping system for compliance with the legislation.
- a test of the client identification procedures for compliance with the legislation.
- a review of the risk assessment.

The scope of the review has to be documented. The scope and details of the review will depend on the nature, size and complexity of your operations. The review process should be well documented and should identify and note weaknesses in policies and procedures. The results of the review also have to be documented, along with corrective measures and follow-up actions.

### **Reporting to senior management**

Effective June 23, 2008, if you are an entity, within 30 days of the review, you have to report the following in writing to one of your senior officers:

- the findings of the above review;
- any updates that were made to the policies and procedures during the review period;
- the status of implementation of the policies and procedures updates.

Any deficiencies should be identified and reported to senior management or the board of directors. This should also include a request for a response indicating corrective actions and a timeline for implementing such actions.

### **Self-review**

If you do not have an internal or external auditor, you can do a “self-review”. If feasible, this self-review should be conducted by an individual who is independent of the reporting, record keeping and compliance-monitoring functions. This could be an employee or an outside consultant. The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

## **9 FINTRAC's Approach to Compliance Monitoring**

FINTRAC has a responsibility to ensure compliance with your legislative requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. To do this, FINTRAC can examine your compliance regime and records. FINTRAC may also periodically provide you with feedback about the adequacy, completeness and timeliness of the information you have reported.

FINTRAC favours a co-operative approach to compliance monitoring. The emphasis will be on working with you to achieve compliance. When compliance issues are identified, FINTRAC intends to work with you in a constructive manner to find reasonable solutions. If this is not successful, FINTRAC has the authority to disclose information related to non-compliance cases to the appropriate law enforcement agencies.

FINTRAC's compliance program will use risk management strategies to identify those most in need of improving compliance. Efforts will be focused on areas where there is greater risk of non-compliance and in which the failure to comply could have significant impact on the ability to detect and deter money laundering and terrorist financing.

Finally, FINTRAC will work with other regulators at the federal and provincial levels to identify areas of common interest and address the potential for overlap in some areas of its responsibilities. In that context, FINTRAC continues to explore avenues for cost efficiencies, consistency of approach and information sharing. Regulators may share information with FINTRAC when they have an agreement to do so.

## 10 Penalties for Non-Compliance

Failure to comply with your legislative requirements can lead to criminal charges against you if you are a person or entity described in section 2. The following are some of the penalties:

- failure to report a suspicious transaction or failure to make a terrorist property report — conviction of this could lead to up to five years imprisonment, to a fine of \$2,000,000, or both.
- failure to report a large cash transaction or an electronic funds transfer — conviction of this could lead to a fine of \$500,000 for a first offence and \$1,000,000 for each subsequent offence.
- failure to retain records — conviction of this could lead to up to five years imprisonment, to a fine of \$500,000, or both.
- failure to implement a compliance regime — conviction of this could lead to up to five years imprisonment, to a fine of \$500,000, or both.

Effective December 30, 2008, failure to comply with your legislative requirements can lead to the following administrative monetary penalties against you if you are a person or entity described in section 2:

- failure to implement any of the five elements of the compliance regime described in section 3 could lead to an administrative monetary penalty of up to \$100,000 for each one.
- failure by an entity to report the required information to senior management within 30 days after the review of its compliance program could lead to an administrative monetary penalty of up to \$100,000.
- failure to identify clients, keep records, monitor financial transactions and take mitigating measures in situations where risk of money laundering or terrorist financing is high could lead to an administrative monetary penalty of up to \$100,000.

For more information on penalties, you can also consult the Penalties for non-compliance section of FINTRAC's Web site.

## 11 Comments?

These guidelines will be reviewed on a periodic basis. If you have any comments or suggestions to help improve them, please send your comments to the mailing address provided below, or by email to [guidelines-lignesdirectrices@fintrac-canafe.gc.ca](mailto:guidelines-lignesdirectrices@fintrac-canafe.gc.ca).

## **12 How to Contact FINTRAC**

For further information on FINTRAC and its activities, and on implementing a compliance regime, please go to FINTRAC's website (<http://www.fintrac-canafe.gc.ca>) or contact FINTRAC:

Financial Transactions and Reports Analysis Centre of Canada  
234 Laurier Avenue West, 24<sup>th</sup> floor  
Ottawa, Ontario  
Canada K1P 1H7

Toll-free: 1-866-346-8722

## Appendix 1: Products, Services, Delivery Channels and Geographic Locations

The following checklist is intended to provide an example of how to assess risk for your products, services, delivery channels and geographic locations. This is only a starting point and you should customize the checklist for your business. Your risk assessment tool has to be appropriate for your specific business needs which means that it may have to be more detailed than this checklist for larger reporting entities, or entities who conduct large volumes of business. If you already use another risk assessment tool, you can continue to use it or enhance it as necessary.

If you answer yes to any of the questions below, you should consider it as higher risk for money laundering or terrorist financing. Where appropriate, risk-mitigation steps should be taken. See subsection 6.2 for more information.

You can also refer to *Guideline 2: Suspicious Transactions* for additional indicators or to the Financial Action Task Force's Web site (<http://www.fatf-gafi.org>) for further guidance on risk-based approach.

Identify whether you provide any of the following products, services or delivery channels	Yes	No	N/A
<b>For all sectors</b>			
Do you offer services that make it difficult to fully identify clients?			
Do you offer electronic funds payment services? Do you offer any of the following: <ul style="list-style-type: none"> <li>• Electronic cash (for example stored value and payroll cards)?</li> <li>• Funds transfers (domestic and international)?</li> <li>• Automated banking machines (ABMs)?</li> </ul>			

Identify whether you provide any of the following products, services or delivery channels	Yes	No	N/A
<b>For financial entities</b>			
<p>Do you offer any of the following:</p> <ul style="list-style-type: none"> <li>• International correspondent banking services involving transactions such as commercial payments for non-clients (for example, acting as an intermediary bank) and use of carriers or couriers for international transport of cash, monetary instruments or other documents (pouch activities)?</li> <li>• Services involving banknote and precious metal trading and delivery?</li> <li>• Electronic banking?</li> <li>• Private banking (domestic and international)?</li> <li>• Foreign correspondent accounts?</li> <li>• Trade finance activities (letters of credit)?</li> <li>• Lending activities, particularly loans secured by cash collateral and marketable securities?</li> <li>• Non-deposit account services (for example, non-deposit investment products and insurance)?</li> <li>• Accounts through which you can extend cheque or bank draft writing privileges to the clients of other institutions, often foreign banks (pass through or payable through type accounts)?</li> <li>• Services involving an immigrant investor program?</li> <li>• Non face-to-face transactions, such as Internet services, by mail or by telephone?</li> </ul>			

Identify whether you deal with clients or provide products or services in the following geographic locations:	Yes	No	N/A
<b>For all sectors</b>			
Is the client located in a known high crime rate area?			
<p>Do you or your clients operate or undertake activities in the following countries:</p> <ul style="list-style-type: none"> <li>• Any country subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN)? In some circumstances, this will include sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized.</li> <li>• Any country identified as a financial secrecy haven or jurisdiction?</li> <li>• Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement? You can consult the current non-cooperative countries and territories listed on the FATF Web site at <a href="http://www.fatf-gafi.org">http://www.fatf-gafi.org</a> (select the “Current NCCT list” tab).</li> <li>• Any country identified by credible sources: <ul style="list-style-type: none"> <li>○ as lacking appropriate money laundering or terrorist financing laws and regulations?</li> <li>○ as providing funding or support for terrorist activities?</li> <li>○ as having significant levels of corruption, or other criminal activity?</li> </ul> </li> </ul> <p>Credible sources means information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly available. Such sources may include, but are not limited to, international bodies such as the World Bank, the International Monetary Fund, the Organisation for Economic Co-operation and Development, and Transparency International as well as relevant national government bodies and non-governmental organisations.</p>			

## Appendix 2: Client and Business Relationships

The following checklist is intended to provide an example of how to assess risk for your client relationships. This is only a starting point and you should customize the checklist for your business. Your risk assessment tool has to be appropriate for your specific business needs which means that it may have to be more detailed than this checklist for larger reporting entities, or entities who conduct large volumes of business. If you already use another risk assessment tool, you can continue to use it or enhance it as necessary.

If you answer yes to any of the questions below, you should consider it as higher risk for money laundering or terrorist financing. Where appropriate, risk-mitigation steps should be taken. See subsection 6.2 for more information.

You can also refer to *Guideline 2: Suspicious Transactions* for additional indicators or to the Financial Action Task Force's Web site (<http://www.fatf-gafi.org>) for further guidance on risk-based approach.

Identify whether any of the following apply to the client:	Yes	No	N/A
<b>For all sectors</b>			
Is the client a cash intensive business? Does the client's business generate large amounts of cash for certain transactions that are not normally cash intensive?			
Is the client an intermediary or "gatekeeper" such as a professional that holds accounts for clients where the identity of the underlying client is not disclosed to you? Does the client use unsupervised intermediaries within the relationship who are not subject to adequate anti-money laundering or anti-terrorist financing obligations?			
Does client identification take place other than face-to-face?			
Does the client reside outside Canada? Does the client deal offshore?			
Is the client an unregistered charity or other unregulated "not for profit" organisation (especially one operating on a "cross-border" basis)?			

Identify whether any of the following apply to the client:	Yes	No	N/A
Is the client located in a known high crime rate area?			
Has the client been identified to have engaged in activity that is consistent with the indicators for your sector identified in <i>Guideline 2: Suspicious Transactions</i> ?			
Does the comparison between your clients with similar profiles and high levels of assets or large transactions seem unreasonable?			
Does the knowledge of local laws, regulations and rules seem excessive for your client?			
Is the client a new client?			
Do your clients use intermediate vehicles (such as corporations, trusts, foundations, partnerships) or other structures that do not seem usual for their business or seem very complex and unnecessary?			
Does the client offer on-line gaming?			
Does the client's structure or nature of its business or relationship make it difficult to identify the true owners or controllers?			
Is there a significant and unexplained geographic distance between you and the location of the client?			
Is there frequent and unexplained movement of accounts or funds between institutions in various geographic locations or to different institutions?			

Identify whether any of the following apply to the client:	Yes	No	N/A
<p>Is the client a politically exposed foreign person?</p> <p>A politically exposed foreign person is an individual who holds or has ever held one of the following offices or positions in or on behalf of a foreign country:</p> <ul style="list-style-type: none"> <li>• a head of state or government;</li> <li>• a member of the executive council of government or member of a legislature;</li> <li>• a deputy minister (or equivalent);</li> <li>• an ambassador or an ambassador’s attaché or counsellor;</li> <li>• a military general (or higher rank);</li> <li>• a president of a state-owned company or bank;</li> <li>• a head of a government agency;</li> <li>• a judge; or</li> <li>• a leader or president of a political party in a legislature.</li> </ul> <p>A politically exposed foreign person also includes the following family members of the individual described above:</p> <ul style="list-style-type: none"> <li>• mother or father;</li> <li>• child;</li> <li>• spouse or common-law partner;</li> <li>• spouse’s or common-law partner’s mother or father and</li> <li>• brother, sister, half-brother or half-sister (that is, any other child of the individual’s mother or father).</li> </ul>			
<b>For financial entities</b>			
Is the client a foreign financial institution with which you have a correspondent banking relationship?			
Is the client a correspondent bank that has been subject to sanctions?			

### Appendix 3: Risk Level Assessment Matrix

You may use the following matrix, as appropriate, when assessing the level of money laundering and terrorist financing risks of your products, services and clients. The following matrix is inspired from a matrix included in a recent document on risk-based approach published by the Financial Action Task Force (FATF).

Low	Moderate	High
Stable, known client base	Client base increasing due to branching, merger, or acquisition	A large and growing client base in diverse geographic area
No electronic transaction services or the Web site is informational or non-transactional	You are beginning electronic transaction services and offer limited products and services.	You offer a wide array of electronic transaction services (i.e., account transfers, or accounts opened via the Internet).
There are few or no large currency transactions.	There is a moderate volume of large currency or structured transactions.	There is a significant volume of large currency or structured transactions.
Identified a few high-risk clients and businesses	Identified a moderate number of high-risk clients and businesses	Identified a large number of high-risk clients and businesses
Few international accounts or very low volume of currency activity in the accounts	Moderate level of international accounts with unexplained currency activity	Large number of international accounts with unexplained currency activity
A limited number of fund transfers for clients, non clients, limited third-party transactions, and no foreign funds transfers	A moderate number of fund transfers, a few international fund transfers from personal or business accounts with typically low-risk countries	Frequent funds from personal or business accounts to or from high-risk jurisdictions, and financial secrecy havens or jurisdictions

Low	Moderate	High
Your business is located in an area known to have low crime rate.	Your business is located in an area known to have moderate crime rate.	Your business is located in an area known to have high crime rate.
No transactions with high-risk geographic locations	Minimal transactions with high-risk geographic locations	Significant volume of transactions with high-risk geographic locations
Low turnover of key anti-money laundering personnel and frontline personnel (i.e., client service representatives, tellers, or other personnel)	Low turnover of key anti-money laundering personnel, but frontline personnel may have changed	High turnover, especially in key anti-money laundering personnel positions