Government of Canada Gouvernement du Canada

Compliance program requirements

Overview

This guidance came into effect on June 1, 2021.

The compliance program requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations **apply to all reporting entities (REs)**.

Who is this guidance for

- All reporting entities (REs)

In this guidance

Related guidance

- Risk-based approach guide

1. What is a compliance program and what are the requirements related to my compliance program?

A compliance program is a program established and implemented by an RE and is intended to ensure their compliance under the PCMLTFA and associated Regulations. A compliance program forms the basis for meeting all of your reporting, record keeping, client identification and other know-your-client requirements under the PCMLTFA and associated Regulations. All REs must establish and implement a compliance program. [1]

Specifically, all REs must implement the following elements of a compliance program by: [2]

- appointing a compliance officer who is responsible for implementing the program;
- developing and applying written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer;
- conducting a risk assessment of your business to assess and document the risk of a money laundering offence or a terrorist activity financing offence (ML/TF) occurring in the course of your activities;
- developing and maintaining a written, ongoing compliance training program for your employees, agents or mandataries, or other authorized persons;
- instituting and documenting a plan for the ongoing compliance training program and delivering the training (training plan); and

- instituting and documenting a plan for a review of the compliance program for the purpose of testing its effectiveness, and carrying out this review every two years at a minimum (two-year effectiveness review).

2. Who can be a compliance officer and what are the responsibilities of a compliance officer?

Depending on the size of your business, you could be the appointed compliance officer, or it could be another individual, such as:

- a senior manager, the owner or the operator of your small business; or
- someone from a senior level who has direct access to senior management and the board of directors of your large business.

If you are a person rather than an entity, such as a sole proprietor, you can appoint yourself as the compliance officer, or you may choose to appoint someone else to help you implement the compliance program.

As a best practice, the appointed compliance officer of a larger business should not be directly involved in the receipt, transfer or payment of funds. The appointed compliance officer should also have independent oversight and be able to communicate directly with those parties who make decisions about the business such as senior management or the board of directors.

Appointing someone to be your compliance officer alone does not fulfil your compliance program requirements. The appointed compliance officer is responsible for implementing all elements of a compliance program. [3] Therefore, a compliance officer needs to:

- have the necessary authority and access to resources in order to implement an effective compliance program and make any desired changes;
- have knowledge of your business's functions and structure;
- have knowledge of your business sector's ML/TF risks and vulnerabilities as well as ML/TF trends and typologies; and
- understand your business sector's requirements under the PCMLTFA and associated Regulations.

A compliance officer may delegate certain duties to other employees. For example, the compliance officer of a large business may delegate responsibility to an individual in another office or branch. However, the compliance officer remains responsible for the implementation of the compliance program.

While the compliance officer is appointed, it is the RE's responsibility to meet its compliance program requirements under the PCMLTFA and associated Regulations.

3. What are the requirements related to my compliance policies and procedures?

Your compliance policies and procedures must be [4]:

- written and should be in a form/format that is accessible to its intended audience;
- kept up to date (including changes to legislation or your internal processes, as well as any other changes that would require an update); and
- approved by a senior officer, if you are an entity.

Your policies and procedures should be made available to all those authorized to act on your behalf, including employees, agents and any others that deal with clients, transactions, or other activities.

Your compliance policies and procedures should cover at minimum the following requirements as applicable to you as an RE:

- **compliance program** requirements: this includes your requirements to have an appointed compliance officer, a risk assessment, an ongoing compliance training program and plan, and a two-year effectiveness review and plan, which consists of a review of your policies and procedures, risk assessment, and ongoing training program and plan;
- **know your client** requirements: this includes your requirements for verifying client identity, politically exposed persons, heads of international organizations, their family members and close associates, beneficial ownership, and third party determination;
- **business relationship and ongoing monitoring** requirements;
- **record keeping** requirements;
- **reporting** requirements;
- **travel rule** requirements: this includes your requirement to develop and apply written risk-based policies and procedures to help determine whether you should suspend or reject an electronic funds transfer (EFT) or virtual currency transfer that you receive, and any other follow-up measures, if the transfer does not include the required travel rule information and you are unable to obtain this information through your reasonable measures; and
- **Ministerial directive** requirements.

Your compliance policies and procedures should also include the processes and controls you have put in place to meet your requirements, including:

- when the obligation is triggered;
- the information that must be reported, recorded, or considered;
- the procedures you created to ensure that you fulfill a requirement; and

- the timelines associated with your requirements and methods of reporting (if applicable).

Your policies and procedures must also describe the steps you will take for all the obligations that require you to take reasonable measures. For example, when you are required to take reasonable measures to obtain information to include in a report, your policies and procedures must describe the steps you will take, which could include asking the client.

If your RE sector has an industry association or governing body that has provided you with a generic set of policies and procedures, you must tailor them to your business.

The level of detail in your compliance policies and procedures will depend on your business's size, structure, and complexity, and degree of exposure to ML/TF risks.

4. What are the requirements related to my risk assessment?

Your compliance program must include policies and procedures that you develop and apply to assess your ML/TF risks in the course of your activities. [5] When assessing and documenting your ML/TF risks, you must consider the following: [6]

- your clients and business relationships, including their activity patterns and geographic locations;
- the products, services and delivery channels you offer;
- the geographic location(s) where you conduct your activities;
- if you are a **financial entity**, **life insurance company**, or **securities dealer**, the risks resulting from the activities of an **affiliate**, if it is also subject to the PCMLTFA and associated Regulations under these RE sectors, or if it is a foreign affiliate that carries out activities outside Canada that are similar to these sectors;

- the risks resulting from new developments or new technologies you intend to carry out or introduce, before doing so, that may have an impact on your clients, business relationships, products, services or delivery channels, or the geographic location of your activities; [7] and
- any other relevant factors affecting your business (for example, employee turnover, industry rules and regulations).

If, at any time, you consider the risk of an ML or TF offence to be high, you must take enhanced measures.

Please see FINTRAC's Risk assessment guidance for further information on risk assessments and risk mitigation.

5. What are enhanced measures?

Enhanced measures are the additional controls and processes that you have put in place to manage and reduce the risks associated with your high-risk clients and business areas. As part of your compliance program, you must develop and apply written policies and procedures for the enhanced measures that you will take for any ML or TF risks you identify as high. [8]

Your policies and procedures for enhanced measures must include: [9]

- the additional steps, based on assessment of the risk, that you will take to verify the identity of a person or entity; and
- any other additional steps that you will take to mitigate the risks, including, but not limited to, the additional steps to:
  - ensure client identification information and beneficial ownership information is updated at a frequency that is appropriate to the level of risk; and
  - conduct ongoing monitoring of business relationships at a frequency that is appropriate to the level of risk.

Enhanced measures to mitigate risk can include:

- obtaining additional information on a client (for example, information from public databases and the internet);
- obtaining information on the client's source of funds or source of wealth;
- obtaining information on the reasons for attempted or conducted transactions; or
- any other measures you deem appropriate.

6. What are the requirements related to my training program and plan?

If you have employees, agents or mandataries, or other persons authorized to act on your behalf, you must develop and maintain a written, ongoing compliance training program. [10] Your training program should explain what your employees, agents or mandataries, or other persons authorized to act on your behalf, need to know and understand, including:

- your requirements under the PCMLTFA and associated Regulations;
- background information on ML/TF, such as the definition of ML/TF and methods of ML/TF;
- how your business or profession could be vulnerable to ML/TF activities (provide indicators and examples);
- the compliance policies and procedures you have developed to help meet your requirements under the PCMLTFA and associated Regulations for preventing and detecting ML/TF, including your reporting, record keeping and know your client requirements; and
- their roles and responsibilities in detecting and deterring ML/TF activities, and when dealing with potentially suspicious activities or transactions.

You must institute and document a plan for your ongoing compliance training program and for delivering the training. [11] Your training plan should cover how you will implement your ongoing compliance training program and its delivery. This includes documenting the steps you will take to ensure your employees, agents or mandataries, or other persons authorized to act on your behalf receive an appropriate level of training relevant to their duties and position, on an ongoing basis. Your training plan should include information about the following:

- training recipients;
- training topics and materials;
- training methods for delivery; and
- training frequency.

Training recipients

Your training plan should explain who will receive training. Training recipients should include those who:

- have contact with clients, such as front-line staff or agents;
- are involved in client transaction activities;
- handle cash, funds, or virtual currency for you, in any way; and
- are responsible for implementing or overseeing the compliance program (such as the compliance officer, senior management, information technology staff or internal auditors).

Training topics and material

Your training plan should outline the topics that will be covered in your training program. It should also include the sources of the training materials that will cover these topics.

Training methods for delivery

Your training plan should describe the training method(s) that you will use to deliver your ongoing compliance training program. Training methods could include self-directed learning (where recipients read materials on their own, register for on-line courses or use e-learning materials), information sessions, face-to-face meetings, classroom, conferences, and on-the-job training where instruction is provided. Instructors can be in-house personnel or an external service provider, but they should have knowledge of the PCMLTFA and associated Regulations. If you decide to use in-house personnel, you may need to hire or allocate staff to provide training. If you decide to use an external service provider, you may need to determine whether their services and training content are suitable for your business. You can use one or more training methods. The method(s) that you choose may depend on the size of your business and the number of people that need to be trained.

Training frequency

Your training plan should describe the frequency of your ongoing compliance training program. Training can be delivered at regular intervals (for example, monthly, semi-annually, annually), when certain events occur (for example, before a new employee deals with clients, after a procedure is changed), or by using a combination of both.

Your ongoing compliance training program and plan should be tailored to your business's size, structure and complexity, and its degree of exposure to ML/TF risk. For example, if you are a large business, you may decide to provide different types of training to your employees, agents or mandataries, or other persons authorized to act on your behalf based on their specific roles and duties (for example, general or specialized training). This should be explained in your training plan.

Your training program should also include a record of the training that has been delivered (for example, the date the training took place, a list of the attendees who received the training, the topics that were covered). Training records will help you keep track of the training and assist you in scheduling the next training dates. They will also demonstrate that you are carrying out your training program on an ongoing basis.

****Note:** If you are a sole proprietor with no employees, agents or other individuals authorized to act on your behalf, you are not required to have a training program nor are you required to have a training plan in place for yourself.

7. What are the requirements related to my two-year effectiveness review and plan?

A two-year effectiveness review is an evaluation that must be conducted every two years (at a minimum) to test the effectiveness of the elements of your compliance program (policies and procedures, risk assessment, and ongoing training program and plan). You must start your effectiveness review no later than two years (24 months) from the start of your previous review. You must also ensure that you have completed your previous review before you start the next review.

The purpose of an effectiveness review is to determine whether your compliance program has gaps or weaknesses that may prevent your business from effectively detecting and preventing ML/TF. Your effectiveness review will help you determine if:

- your business practices reflect what is written in your compliance program documentation and if you are meeting your requirements under the PCMLTFA and associated Regulations.

- your risk assessment is effective at identifying and mitigating the ML/TF risks related to your clients, affiliates (if any), products, services, delivery channels, new developments or technology, and geographic locations where you do business.

The review must be carried out and the results documented by an internal or external auditor, or by yourself if you do not have an auditor. [12] Your review should be conducted by someone who is knowledgeable of your requirements under the PCMLTFA and its associated Regulations. Also, as a best practice, to ensure that your review is impartial, it should not be conducted by someone who is directly involved in your compliance program activities. Regardless of who carries out the review, as an RE it is your responsibility to ensure that the review is conducted (at a minimum) every two years and that the review tests the effectiveness of your compliance program.

You must also institute and document a plan for the two-year effectiveness review of your compliance program. [13] This plan should describe the scope of the review and must include all the elements of your compliance program. The breadth and depth of review for each element may vary depending on factors such as the complexity of your business, transaction volumes, findings from previous reviews, and current ML/TF risks. Your plan should not only describe the scope of the review, but it should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods and sample sizes.

The evaluation methods can include, but are not limited to, interviewing staff, sampling records and reviewing documentation. The following are examples of what can be included in your review:

- interviews with those handling transactions to evaluate their knowledge of your policies and procedures and related record keeping, client identification and reporting requirements;

- a review of a sample of your records to assess whether your client identification policies and procedures are being followed;
- a review of your agreements with agents or mandataries, as applicable, as well as a review of a sample of the information that your agents or mandataries referred to in order to verify the identity of persons, to assess whether client identification policies and procedures are being followed;
- a review of transactions to assess whether suspicious transactions were reported to FINTRAC;
- a review of large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines;
- a review of electronic funds transfers to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to RE sectors that have EFT obligations);
- a review of a sample of your client records to see whether the risk assessment was applied in accordance with your risk assessment process;
- a review of a sample of your client records to see whether the frequency of your ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment;
- a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken;
- a review of a sample of your records to confirm that proper record keeping procedures are being followed;
- a review of your risk assessment to confirm that it reflects your current operations; and
- a review of your policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect your current business practices.

You should also document the following in your two-year effectiveness review:

- the date the review was conducted, the period that was covered by the review and the person or entity who performed the review;
- the results of the tests that were performed; and
- the conclusions, including deficiencies, recommendations and action plans, if any.

If you are an entity, you must report, in writing, the following to a senior officer no later than 30 days after the completion of the effectiveness review: [14]

- the findings of the review (for example, deficiencies, recommendations, action plans);
- any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself; and
- the status of the implementation of the updates made to your policies and procedures.

Details and history

Published: May 2021

For assistance

If you have questions about this guidance, please contact FINTRAC by email at guidelines-lignesdirectrices@fintrac-canafe.gc.ca.

1 Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c 17, s. 9.6(1).

2 Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 156(1).

3 PCMLTFR, SOR/2002-184, s. 156(1)(a).

4 PCMLTFR, SOR/2002-184, s. 156(1)(b).

5 PCMLTFA, S.C. 2000, c 17, s. 9.6(2).

6 PCMLTFR, SOR/2002-184, s. 156(1)(c).

7 PCMLTFR, SOR/2002-184, s. 156(2).

8 PCMLTFA, S.C. 2000, c 17, s. 9.6(3).

9 PCMLTFR, SOR/2002-184, s. 157.

10 PCMLTFR, SOR/2002-184, s. 156(1)(d).

11 PCMLTFR, SOR/2002-184, s. 156(1)(e).

12 PCMLTFR, SOR/2002-184, s. 156(3).

13 PCMLTFR, SOR/2002-184, s. 156(1)(f).

14 PCMLTFR, SOR/2002-184, s. 156(4).

Date Modified:
2021-11-19