Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

FINTRAC

Assessment Manual

The approach and methods used during examinations

Canada

Table of contents

May 2023

Introduction

Why is the manual important and what does it cover?

The Financial Transactions and Reports Analysis Centre of Canada, known as FINTRAC, is committed to helping you meet the legal requirements set out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

Our objective is to support businesses as we work together to protect Canadians and the integrity of Canada's financial system from money laundering and terrorist activity financing vulnerabilities.

To this end, in the spirit of openness and transparency, we have published this assessment manual detailing how we conduct examinations.

Examinations are one of the main activities we use to assess whether businesses are adequately implementing and maintaining a compliance program, which is important to detecting and mitigating the money laundering and terrorist activity financing risks your business may face. In turn, it can also reduce financial, reputational and legal risks should criminals try to exploit your business's vulnerabilities.

The manual does not replace the PCMLTFA and associated Regulations, establish new legal requirements or expectations, serve as regulatory guidance, or tell you how to carry out your day-to-day business operations.

The manual, which is for all Canadian businesses covered by the PCMLTFA, describes how FINTRAC conducts its compliance examinations. It is meant to help you understand how we assess whether you have implemented and maintained a compliance program that adequately meets all of the legal requirements, and to help you prepare for a FINTRAC examination.

The manual is divided into three parts:

1. Part 1—the framework we apply to ensure that we conduct our examinations in a consistent manner;
2. Part 2—the phases of an examination; and
3. Part 3—the methods we use in examinations to assess whether you are adequately meeting the legal requirements.

While our examinations take into account the differences across business sectors, our overall examination approach and methods remain the same for all.

The assessment methods we may use in an examination are not limited to those described in the manual. The manual is an evergreen document that we will update through consultations with businesses as our assessment methods evolve, or as legislative and regulatory changes are introduced.

The manual represents FINTRAC's examination approach and methods. It does not address how other federal or provincial regulators or supervisors carry out their oversight activities relating to compliance with anti-money laundering and anti-terrorist activity financing requirements.

Note: FINTRAC typically refers to the businesses covered by the PCMLTFA as reporting entities, while the PCMLTFA refers to "persons" and "entities". In this manual, the term "businesses" will be used.

Part 1—Examination framework

The examination framework we use ensures that we conduct our examinations in a consistent manner, while taking into account the type, nature, size, and complexity of different businesses.

The framework is comprised of three main components outlined below.

Risk-based examinations

We focus our examinations on areas where your business may be vulnerable to money laundering or terrorist activity financing risks and where there is a greater risk of not meeting the legal requirements (risk of non-compliance). Using this approach reduces the burden on businesses by minimizing disruptions and ensuring the effective and efficient use of resources.

When determining the risks your business may be exposed to, we rely on our experience, knowledge, training, and professional judgment. We take into account relevant information from FINTRAC publications and guidance. We may also take into consideration relevant information taken from publicly available reports and publications issued by well-known credible sources on money laundering and terrorist activity financing.

We recognize that businesses will adopt different approaches to implementing and maintaining their compliance programs, based on their type, nature, size, complexity and risk profile. In light of this, we will include in our examination plans the areas you have identified as posing a higher risk to your business as well as gaps you have identified in your compliance program, where appropriate.

Part 2 of the manual describes in more detail how risk informs our examinations.

Assessment methods

Once we have evaluated your business's risks, we select assessment methods described in Part 3 that we will use as part of our examination.

We use the methods to assess how you comply with the legal requirements set out in the PCMLTFA and associated Regulations. We also consider FINTRAC guidance, which sets out how we interpret the legal requirements.

For example, the PCMLTFA requires that Suspicious Transaction Reports be submitted to FINTRAC under certain circumstances. FINTRAC guidance presents money laundering and terrorist activity financing indicators to help businesses better understand typical risks they may be exposed to, and should watch for, in their day-to-day activities. When we assess the requirement to report suspicious transactions using the methods described in the manual, we may refer to the indicators we provide in the guidance, in addition to the obligation in the PCMLTFA, to support the rationale for suspicion.

When applying our assessment methods, we may review your documents, client records, records of transactions, and financial transaction reports, as well as conduct interviews.

Assessment approach to evaluating findings

We take an assessment approach when evaluating examination findings. This means that we take a holistic approach when evaluating findings rather than evaluating them in isolation. We focus less on technical non-compliance and more on the overall soundness of the areas of your compliance program we are assessing.

We look at all the information gathered to ensure that your compliance program is complete and put into practice. When we identify technical non-compliance within an otherwise adequate system of policies, procedures, processes, and controls, we will notify you of the non-compliance, but the overall result of our assessment may not be negatively affected by it.

With our findings, we aim to make decisions that are reasonable, fair, and balanced. We base our decisions on what we believe a reasonable, experienced

and knowledgeable person in your business sector would have done if they were assessing the same set of facts and circumstances.

We expect you to provide us with, or make available, all relevant facts and information so that we can make decisions based on complete information.

Finally, in the spirit of transparency, openness, and fairness in our examinations, we will share our findings with you during the examination, explain them, and offer you the opportunity to provide us with additional information for our consideration.

Part 2—Examination phases

Examinations are conducted on weekdays, during FINTRAC's regular business hours (8 a.m. to 5 p.m.). If these hours do not suit your business, please notify us, as we may be able to offer some flexibility.

The number of days we will spend on your premises will depend on the type, nature, size, and complexity of your business. For example, the examination of a small or medium-sized business may take less than a week, while the examination of a bank may take several weeks.

In order to ensure the examination runs efficiently, and to reduce unnecessary business disruptions, it is important that you provide us with the requested information, documents, client records, records of transactions, and access to your staff, for interview purposes, in a timely manner.

Our examinations are broken down into three phases: planning and scoping; examination and assessment; and developing the findings and finalizing the examination. Below, we present each phase and describe the roles and responsibilities of each party to an examination.

Roles and responsibilities

You can expect us to be professional, provide clear information, respect your privacy and the confidentiality of your clients' personal and financial information, and offer services in either official language. You can also expect us to observe the highest standard of ethical conduct.

The PCMLTFA requires FINTRAC to protect the personal information under its control. We take this mandate very seriously and safeguard all personal information when we carry out an examination.

The PCMLTFA also requires that you provide FINTRAC with assistance during an examination. This assistance includes providing us with the information we ask for within the agreed upon timelines, giving us access to your place of business, providing us with the documents and records we request, answering our questions about your business and making employees available for interviews. We may also ask you to assist us in accessing information stored on your computers and systems, to help us better understand your operations.

Phase 1—Planning and scoping

Once we select a business for examination, we begin planning the examination, which includes selecting the areas and requirements we will examine (examination scope), as well as the assessment methods we will use.

Planning the examination

We develop the overall plan to determine the staffing needs and level of expertise required to conduct the examination based on the type, nature, size, and complexity of the business to be examined.

Setting the scope of the examination

When we set the scope of the examination, we choose the business areas and the specific requirements that we will examine.

To do this, we first gain a general understanding of your business model, environment, activities and operations. We then look at the risks your business may be exposed to, as well as the risks associated with your business sector. This includes determining:

i. your business areas at risk of being used for money laundering and terrorist activity financing; and

ii. your business areas at risk of not meeting the legal requirements of the PCMLTFA and associated Regulations (the risk of non-compliance).

In order to gather this information and assess your risk, we may consult the files we have on your business and search the internet. For example, we may look at, as applicable:

- Your history of compliance with the PCMLTFA and associated Regulations;
- Findings from previous FINTRAC examinations or examinations conducted by a regulator or supervisor with whom FINTRAC has established a Memorandum of Understanding (MOU) to share information related to compliance with the PCMLTFA;

- Letters and emails you may have sent us describing how you will address previously found non-compliance;
- Voluntary self-declarations of non-compliance (VSDONC) in which you informed us that you have not met certain requirements;
- Previous questions you asked about the requirements or requests for policy interpretations to ensure that potential non-compliance has been addressed in a reasonable period following the enquiries (if applicable);
- Financial transaction reports you sent to FINTRAC;
- Actions taken when you received feedback from us about the quality, timing or volume of your financial transaction reports;
- Policies and procedures, risk assessments and two-year reviews and other documents and information that we may have on file from a previous examination;
- Information about your business or your clients available on the internet; and
- History of enforcement actions (administrative or criminal), in respect of your business, taken by FINTRAC, other regulatory/supervisory bodies, and law enforcement.

We use this information to assess risk and determine the scope of the examination, including the requirements we will assess and the appropriate assessment methods we will use. We also use a risk-based approach to establish the number of sample documents, client records, records of transactions, and financial transaction reports we plan to examine, the period covered by the examination, and who will be interviewed from your business.

When we have limited information on file regarding a business, we rely on the characteristics of similar businesses, and on the information obtained in our examination notification call to define the scope of the examination.

Desk versus on-site examinations

We conduct examinations either remotely (a desk examination), or at your place of business (an on-site examination). You will be informed of the examination's location during our notification call and in the notification letter.

In either case, you must send all the requested information, documents and records to FINTRAC for a preliminary review.

When we conduct an examination remotely, we hold interviews with your compliance officer, employees, and agents (if applicable). When we conduct our examination at your place of business, we typically hold in-person interviews at your main location and may visit or call your other locations, if applicable, to conduct our interviews.

If you have multiple business locations, we typically ask that the information, documents, and records from all your locations be made available for our review at the location that has been selected for the examination.

Examination notification

We will call the person responsible for the implementation of your compliance program (commonly referred to as the compliance officer) to discuss an upcoming examination's scope and date.

After our notification call, we will confirm the examination details in writing with a notification letter addressed to your compliance officer. The letter will indicate where and when we will conduct the examination. We will usually send you the letter 30 to 45 days before the examination date. Given the amount of information and data involved, we may provide larger businesses with more than 45 days' notice to grant them sufficient time to gather the required information.

The letter is our formal request for information, documents and records, and for your assistance during the examination. We will ask you to send the requested material to FINTRAC, including, for example, your compliance program documents and when applicable, lists of transactions and records of transactions.

While we always encourage businesses to address non-compliance whenever they detect it, we will not generally accept certain documents, records, or financial transaction reports once an examination has started.

If you identify non-compliance *after* a FINTRAC examination has started, you should inform the FINTRAC officer immediately and send us a voluntary self-declaration of non-compliance. We consider the date on which we notify you of the examination to be the start of the examination (that is, the date of the notification call).

When we receive a voluntary self-declaration of non-compliance on an issue that was not previously voluntarily disclosed *before* a FINTRAC examination has started, we will not consider enforcement actions, such as an administrative monetary penalty. However, if we receive a self-declaration *during* an examination, we will assess the non-compliance as part of the examination, work with the business to correct it, and determine if the non-compliance warrants an enforcement action.

For example, if you did not submit a financial transaction report to FINTRAC when required and then submit it after the notification date, we will consider that you did not meet your requirement to submit the report. In addition, there may be situations where compliance program documents (for example, compliance policies and procedures) are created or adjusted after the notification date. In such cases, we may determine that you did not meet the compliance program requirements.

When we ask you to send us documents, client records and transaction records in advance of the examination, we do so to conduct the examination more efficiently and to minimize any disruption to your business during the on-site examination.

While we request most of the documents that we will need during the planning phase, we may request additional information or documents at a later stage of the examination process.

Given the sensitive nature of the documentation, and in the interest of limiting the risk of loss during transit, we encourage you to provide the material electronically through a secure digital mailbox service. This type of service uses

advanced encryption that allows for the transmission of sensitive information securely. If you agree to use this option, please contact FINTRAC for further information on the process.

Reviewing the material you send us

We will review the material we requested in our notification letter, including your compliance program documents. This material is used to help us prepare interview questions. It may also further inform the scope of our examination. If the scope of the examination changes, we will notify you.

Phase 2—Examination and assessment

In this phase, we apply the assessment methods described in Part 3.

We start by conducting a preliminary assessment of the requirements that were part of the initial examination scope. We review your documents, conduct preliminarily interviews with your compliance officer, employees, or agents and review a sample of your transaction records and financial transaction reports. The objective of this preliminary assessment is to determine areas where we need to focus our attention.

If we identify areas or issues that require further attention, we will sample more client records, transaction records and reports, and if required, conduct follow-up interviews with your compliance officer, employees or agents. This may lead us to broaden the scope of the examination. If we need to adjust the scope of the examination, you will be notified.

This phase of the examination may extend beyond our last day on your premises or beyond the date of our videoconference or telephone interviews for desk examinations. This may be necessary if we need to further review and analyze certain documents, client records, transaction records, and reports before we consolidate our findings.

Conducting interviews

We may interview different members of your staff and your agents. These one-on-one interviews may be in person, by telephone or both.

We do our best to minimize undue business disruptions, particularly as they relate to front-line business functions. We also make every effort to make employees feel at ease.

We do not expect interviewees to memorize your business's policies and procedures or other documents. Rather, our goal is to confirm that your employees and agents are aware of the requirements applicable to their duties and know how to seek clarification when needed.

Exit meeting

Even if we need to continue our review, once we are ready to leave your premises or have concluded the desk examination, we will hold an exit meeting in person, by telephone, or videoconference to discuss our preliminary findings with you. The findings are presented as “deficiencies”. Each deficiency is a violation of a provision in the PCMLTFA or associated Regulations.

At this time, you may offer additional information to help clarify a deficiency. We will agree on a timeline for you to provide this material. After our review of this material, we may maintain our original deficiency, modify it, or withdraw it.

Phase 3—Developing conclusions and finalizing the examination

Deciding on our findings

When we consolidate our findings, we use the assessment approach described in Part 1. Using this approach, we focus less on technical non-compliance and more on the overall soundness of the areas of your compliance program we are assessing. We evaluate findings holistically, rather than in isolation, to determine if you are adequately meeting the requirements.

As part of our evaluation, we consider the harm done by not meeting a requirement. In doing so, we assess the nature, relative importance, extent, the root cause of the non-compliance, and any mitigating or aggravating factors.

The nature of the non-compliance means which requirement (such as a compliance program or financial transaction reporting requirement) was not met.

We consider the relative importance of the requirement with which you were not compliant. While all requirements are important, and we expect businesses to fulfill them, certain requirements have a greater impact on FINTRAC's ability to carry out its mandate and on Canada's anti-money laundering and anti-terrorist financing regime. For example, the requirement to submit financial transaction reports could have a greater impact on FINTRAC's intelligence mandate and the regime as a whole than the requirement to submit reports that are free of minor data-quality issues.

We also assess the extent (degree) of the non-compliance; that is, how much information is missing from a required document, record or financial transaction report; how many times the non-compliance is repeated; and if the non-compliance points to gaps in the compliance program. We also try to identify the root cause of the non-compliance.

We look at all of the information we have gathered to ensure that your compliance program is complete and put into practice. When we identify technical non-compliance within an otherwise adequate system of policies, procedures, processes, and controls, we will make note of the non-compliance, but the overall results of our assessment may not be negatively affected by it.

Finally, we take into account other mitigating or aggravating factors that may influence how we view the non-compliance. Mitigating factors may decrease the seriousness of the non-compliance, while aggravating factors may increase it. For example, a business may have submitted a Suspicious Transaction Report (STR), but omitted to send a Large Cash Transaction Report (LCTR) that was also required. If most of the LCTR's information is included in the STR, we may consider this a mitigating factor.

Examination findings letter

We will send our examination findings letter to your compliance officer. This letter describes the findings that we discussed during the exit interview.

The letter will indicate the documents, client records, transaction records and financial transaction reports we have examined, as well as the consolidated results of our interviews with your employees and agent. When applicable, we will provide additional information, such as the number of documents we sampled and the number of instances of non-compliance that were found in the sample. The individual records and reports that we have found to be deficient will be listed in an annex to the letter.

In some cases, the letter may also include "observations". They are included to help you improve your business processes and practices in order to strengthen your compliance program.

The letter will also state which of the following three actions we may take following an examination based on the results of our assessment:

- no further compliance or enforcement action;
- possible follow-up compliance action; or
- a recommendation for an enforcement action, such as an administrative monetary penalty (AMP).

When you receive a findings letter, we expect you to address the causes of the identified deficiencies within a reasonable amount of time. In certain cases, we may ask you to send us an action plan that describes how and when the cause of the deficiencies will be addressed. When requested, an action plan must be

sent within 30 calendar days of the receipt of the findings letter, unless otherwise specified. When an action plan is not requested, we still expect that you will take the time to address the cause of the deficiencies. Whether an action plan has been requested or not, you do not need to send us documents that demonstrate that the deficiencies have been addressed. We will evaluate these documents should we conduct a follow-up compliance activity.

If, on the basis of the examination findings, FINTRAC is considering issuing an administrative monetary penalty, this will be stated in the findings letter. The findings letter will also inform you how many days you have to send us any additional information, which is generally 30 calendar days, that you believe could influence our findings or our decision to issue an administrative monetary penalty. We will take into consideration additional relevant information you provide us within the established timeline and send you a written response of our decision. In cases where any adjustment to the findings is required, our response will include a revised findings letter.

Follow-up activities

After an examination, we may follow up to make sure that you have addressed the deficiencies we identified in our findings letter. We may:

- Conduct a follow-up on-site or desk examination;
- Monitor the reports you send to FINTRAC, if the examination revealed that the quality of your reports was inadequate or that the reports were late; and
- Monitor the progress of your action plan, if we asked you to provide one.

Penalties for non-compliance

Our focus is on supporting businesses—administrative monetary penalties are not meant as an automatic response to non-compliance. If we decide to impose a penalty, our aim is to encourage a change in compliance behaviour. When deciding whether a penalty should be considered, FINTRAC compliance officers assess the harm done by looking at various factors. They will assess the nature, relative importance, extent, and root cause of the non-compliance, mitigating

or aggravating factors, and a business's history of compliance. Generally speaking, penalties may be issued in cases of serious or repeated non-compliance. We will consider the unique factors in each case to determine if the examination should result in a penalty.

Should you receive a penalty, you have the right to make representations to FINTRAC's Director and Chief Executive Officer (CEO) for the review of your file. You also have the right to appeal the Director and CEO's decision to the Federal Court. Please visit our administrative monetary penalties page for more information.

We may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance, and where there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting an offence arising out of a contravention of Part 1 or Part 1.1 of the PCMLTFA (related to non-compliance). It is then up to law enforcement to conduct an investigation and decide whether further action is warranted. Please visit our penalties for non-compliance page for more information.

Part 3—Assessment methods

In Part 3, we describe the assessment methods that we use to ensure that you are adequately meeting the requirements.

We use the methods to assess how you comply with the legal requirements set out in the PCMLTFA and associated Regulations. We also consider FINTRAC guidance, which sets out how we interpret the legal requirements.

We assess the following requirements, unless exemptions apply:

- compliance program requirements;
- client identification and other know your client requirements;
- financial transactions reporting requirements;
- record keeping requirements;
- correspondent banking relationship requirements;
- foreign branches, foreign subsidiaries and affiliates requirements;
- registration of money services business and foreign money services business requirements; and
- ministerial directives' requirements.

We may not assess all of the requirements listed above during an examination, nor will we use every assessment method described in this section. Instead we will choose the requirements and the assessment methods that best fit our risk assessment of your business and the scope of the examination.

In the interest of efficiency, we may apply some of our assessment methods simultaneously, or use variations of the methods described in this section.

3.1. Compliance program requirements

This section describes the methods we use to assess whether you have adequately implemented and maintained a compliance program.

The five required elements of a compliance program are to:

- appoint a compliance officer;
- develop policies and procedures;
- conduct a risk assessment;
- develop and provide an ongoing compliance training program; and a plan for the delivery of the program; and
- develop a plan to conduct an effectiveness review of the compliance program, and carry it out every two years.

We will verify that you have a well-documented and complete compliance program in place, and assess whether your compliance program is put into practice.

To do so, we assess your compliance with other requirements, such as client identification and other know your client requirements, reporting requirements, and record keeping requirements. We may consider deficiencies identified through the assessment of these other requirements to be an indication that one or more of the five elements of your compliance program is not being applied.

3.1.1. Compliance officer—the person responsible for the implementation of the compliance program

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to appoint a compliance officer who is responsible for implementing your compliance program.

We verify that the following criteria have been adequately met: appointment (selection), authority, knowledge, and duties.

To conduct this assessment, we may:

- Review documents that show you have formally appointed a compliance officer. We may also review your compliance officer's job description, documents that describe their authority, and an organizational chart. We may also review your policies and procedures to confirm that they give your compliance officer enough guidance to meet the legal requirements.
    - Confirm that the compliance officer has direct access to senior management or the board of directors, to those who make important decisions about compliance issues or who control the company (where applicable).
    - Confirm that the compliance officer has timely access to information from all business lines to ensure they have knowledge of and are aware of potential compliance related risks or concerns (where applicable).
- Look at the compliance officer's background and experience, as well as the training you have given them to verify that you have made sure that the officer has enough knowledge of:
    - your business's functions and structure;
    - your sector's money laundering and terrorist activity financing risks and vulnerabilities, as well as related trends and typologies; and
    - your sector's requirements under the PCMLTFA and associated Regulations.

Our focus

While we assess the appointment, authority, knowledge and duties of the compliance officer, our focus is on verifying that the compliance officer is fulfilling their duties to implement a sound compliance program. To make this determination, we assess whether the areas of your compliance program that we examined are adequately put into practice.

3.1.2. Policies and procedures

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to develop, document and apply policies and procedures.

We verify that your policies and procedures cover requirements such as (if applicable, and not meant to be exhaustive):

- compliance program, including special measures you take for high risk;
- client identification and other know your client requirements;
- financial transactions reporting;
- record keeping;
- correspondent banking relationships;
- foreign branches, foreign subsidiaries and affiliates;
- registration of money services businesses and foreign money services businesses;
- travel rule;
- reasonable measures; and
- ministerial directives.

We also verify that your policies and procedures include the processes and controls you have in place to implement your policies and meet your requirements. For example:

- The process you have in place and the source you use to convert foreign currency and virtual currency into Canadian dollars to meet your reporting, verifying identity and record keeping obligations when an exchange rate is not published by the Bank of Canada.
- The processes you have in place to take reasonable measures to obtain and report information.

- The process you have in place to establish reasonable grounds to suspect that transactions or attempted transactions may be related to money laundering or terrorist activity financing, and your process for submitting Suspicious Transaction Reports "as soon as practicable" and as a priority over other tasks.
- The process you have in place for electronic funds transfer and virtual currency transfers to meet your travel rule obligations. We will also review the process you follow when, after taking reasonable measures, you are unable to obtain the required information and the steps that you take to decide whether you allow, suspend or reject a transaction, and any follow-up measures you take.

We also verify that your policies and procedures are adequate, tailored to your business (that is, they take into account the type, nature, size, and complexity of your business) and are designed to control the risks you may face.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they are written, up to date and, if your business is an entity, approved by a senior officer.
- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Interview your employees and agents to assess their knowledge of your policies and procedures.

Our focus

While we assess your policies and procedures, we will focus on ensuring that you are adequately putting them into practice with respect to your obligations, including reporting, client identification, beneficial ownership, third party determination, politically exposed persons and heads of international organizations, ministerial directives, and special measures for high-risk client requirements, when required.

3.1.3. Risk assessment

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to assess and document your business risks and vulnerabilities related to money laundering and terrorist activity financing.

We verify that you have a documented risk assessment and that it includes the following elements, as applicable: products, services and delivery channels; clients and business relationships; geographic locations; new developments and new technologies; foreign and domestic affiliated entities (if applicable), and other prescribed high-risk elements such as persons or entities listed in ministerial directives.

We also verify that your risk assessment takes into account the type, nature, size, and complexity of your business, and we consider the rationale for each element of your business risk assessment.

To conduct this assessment, we may:

- Verify that you have assessed and documented the risks to your business related to money laundering and terrorist activity financing and that you have identified measures to mitigate these risks, and applied special measures for any high risks.
- Verify that you have assessed and documented risk using a risk-based approach before you implement a new development or introduce a new technology that may affect your clients, business relationships, products, services or delivery channels, or the geographic location of your activities. We may also review the process you follow before introducing new developments or new technologies.
- Verify that you have assessed risks adequately by looking at the areas you have identified as posing a high-risk and the assessment's written rationale. We may review a sample of client records and transaction records in order to determine whether your risk assessment is reasonable and consistent with your business's risk profile, and policies and procedures.

- Verify that you document and apply special measures to elements you have determined pose a high risk. Special measures include taking enhanced measures to identify clients and to mitigate risks such as keeping client identification information up to date and conducting ongoing monitoring for the purpose of detecting suspicious transactions, as well as any other enhanced measures you identify.
- Verify that the controls you have in place are consistent with your identified risk levels (ratings or rankings) and adequately mitigate your business risks.
- Verify that your compliance program is in line with and informed by the results of your risk assessment. For example, we will confirm that your policies and procedures, ongoing training documentation and two-year review documentation adequately address the areas you have assessed as posing a higher risk and that they provide adequate guidance to your employees or agents.
- Verify how you use publicly available information to inform your compliance program.
- Interview the employees and agents responsible for your risk assessment to assess their knowledge of the requirements associated with conducting a risk assessment.

Our focus

While we review the elements of your risk assessment, we will focus on verifying that you have considered and rated the risk of all aspects of your business, that you have provided rationales for your decisions, and that you have applied special measures to areas identified as posing a high risk.

3.1.4. Ongoing compliance training program and plan

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to develop and maintain a written, ongoing compliance training program for employees, agents, and those acting on your behalf. We will also assess your compliance with the requirement to have a documented plan to deliver your training program on an ongoing basis.

We look at who receives training, what topics are covered, when and how often training takes place, how you have implemented your training program, and how training is delivered.

We also verify that your training program is adequate, takes into account the size, type, nature and complexity of your business, and is put into practice.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance to your employees, agents, and those acting on your behalf to develop, implement and maintain an ongoing training program.
- Review your training plan to confirm that it considers and documents the steps you take to develop, maintain, and deliver your training program.
- Review your training material to confirm that the training content is suitable. For example, we verify that it is tailored to your business and adequate for your employees, agents and their respective responsibilities.
- Interview your employees and agents to confirm that they understand the requirements as they relate to their positions, understand and follow the policies and procedures, understand how your business could be vulnerable to ML/TF activities, and have received adequate ongoing training.

Our focus

While we assess your ongoing training program, we will focus on whether it helps your employees and agents understand the requirements, your policies and procedures, and indicators and trends of money laundering and terrorist activity financing. We will also pay close attention to the training you provide regarding the detection of suspicious transactions.

3.1.5. Two-year effectiveness review

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to institute and document a review of the compliance program to test its effectiveness.

We will verify that you have a documented plan to conduct a review of your policies and procedures, risk assessment, and training program for the purpose of testing their effectiveness, and that you carry out this plan to conduct a review every two years.

We will verify that your two-year effectiveness review is adequate, tailored to your business by taking into account the type, nature, size, and complexity of your business, and consistent with your risk assessment.

To conduct this assessment, we may:

- Review your documented plan to verify that it considers all the elements of your compliance program for the purpose of testing its effectiveness.
- Review your policies and procedures to determine whether they give enough guidance to your employees or agents to conduct a two-year effectiveness review.
- Look at the scope of the review (what the review covered) and methodology (how the review was conducted):
    - Interview the person who conducted the review to learn about its scope and methodology, and to ensure that they understand all the requirements that apply to your business;
    - When looking at the scope, for example, we assess whether your policies and procedures, risk assessment and ongoing compliance training program have been reviewed and cover the current legal requirements and your current operations. We also confirm that the review covers and tests all the requirements applicable to your sector; and

    - When looking at the methodology, for example, we verify whether the review was carried out by an internal or external auditor, or by you if you do not have an auditor; whether it was conducted within the required timelines; and whether the testing methods and methodology used were adequate and reasonable.

- Verify that a written report has been provided to a senior officer within 30 days after the completion of the review, and that the report includes the findings of the review, updates made to the policies and procedures within the reporting period of the review, and the status of the implementation of these updates.
- Verify that the findings of the review are being actioned.

Our focus

We verify that your review assesses whether you have a well-documented compliance program and that your program is adequately put into practice. We will also focus on whether your review adequately identifies areas where you did not meet your requirements, whether you updated your policies and procedures, and the status of these updates.

3.2. Client identification and other know your client requirements

We use the methods described in this section to assess your compliance with client identification and other know your client requirements.

3.2.1. Client identification requirements

(Applicable to all business sectors)

To conduct our assessment of your compliance with the verifying client identity requirements we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to verify the identity of your clients.
- Review client records and transaction records to confirm that you apply these policies and procedures.
- Confirm, through a review of client records and transaction records, that you verify the identity of persons and entities in all situations where you are required to do so. These situations include, but are not limited to, when you:
    - open an account for a client, if applicable;
    - receive cash or virtual currency in the amount of $10,000 or more from, or on behalf of, the same person or entity within a 24-hour period;
    - must submit a Suspicious Transaction Report;
    - must create an information record; and
    - are unable to obtain or confirm beneficial ownership information and must therefore take reasonable measures to identify the most senior managing officer of the entity.
- Verify that you use the methods prescribed by law to verify the identity of a person or an entity and that you rely on valid and current information, or authentic, valid and current documents to do so.

- Confirm that you verify the identity of your clients within the prescribed timeframe.
- Interview your employees and agents to assess their knowledge of verifying client identity requirements.

If you use an agent, another reporting entity, or a foreign affiliated entity to help you verify the identity of clients, we may:

- Verify that you have a written agreement with the agent, reporting entity, or the foreign affiliate.
- Verify that you obtain all the required information from the agent, reporting entity, or the foreign affiliate as soon as feasible.
- Verify how you ensure that your agent, reporting entity, or foreign affiliate is using the identity verification methods required by law.

In addition, we verify that you document the required information when you verify the identity of a person or an entity. Refer to our record keeping guidance for more information on the requirement to keep records and to the section of this manual that describes the methods we use to assess record keeping.

When you have verified the identity of a client as required by the PCMLTFA and associated Regulations, you may have additional responsibilities related to know your client requirements. Refer to our know your client guidance and to the section of this manual that describes the methods we use to assess these requirements for more information.

Our focus

We will focus on the steps you take to ensure that you verify the identity of a person or an entity.

3.2.2. Know your client requirements

We use the methods described in this section to assess your compliance with the know your client requirements, including:

- Business relationships and ongoing monitoring requirements;
- Beneficial ownership requirements;
- Third party determination requirements (based on specific activity)
- Politically exposed persons and heads of international organizations requirements (based on specific activity).

To assess the requirements listed above, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Review your client records and transaction records to confirm that you put the policies and procedures into practice.
- Review records of transactions to confirm that you take the necessary steps for all the know your client requirements (as applicable) including:
    - taking all the measures as described in the know your client guidance;
    - obtaining the required approvals;
    - identifying your clients;
    - obtaining and keeping records of required information;
    - performing a risk assessment and ongoing monitoring;
    - taking special measures when required; and
    - meeting the requirements within the prescribed timeframes.
- Interview your employees and agents to assess their knowledge of the know your client requirements.

We use the methods listed below to evaluate your risk assessment practices relating to knowing your client.

Business relationships and ongoing monitoring

To conduct this assessment, we may:

- Verify that you used the results of your risk assessment to determine how often you monitor your clients, or which transactions you will monitor more often or more closely. We focus on situations where you may not be adequately monitoring a client or transactions that you consider to pose a high-risk or to be suspicious.
- Verify that you monitor your high-risk business relationships more frequently to identify suspicious transactions, and apply special measures to mitigate risks.
- Review business relationships that you have ranked as posing a low or medium risk to determine whether this ranking is appropriate. We will compare your low-risk and medium-risk clients to your high-risk clients in light of the criteria you have established to identify high-risk situations.
- Review your ongoing monitoring of low and medium risk business relationships to ensure they are adequately monitored.
- Verify that you identify and address inconsistencies between a client's actual and expected transactional activity. Transactional activity inconsistency is a common indicator of money laundering and terrorist activity financing.

Beneficial ownership

To conduct this assessment, we may:

- Verify that you have a process in place to obtain beneficial ownership information.
- Verify your records and the process you have in place to confirm the accuracy of the information obtained.
- Verify whether you take reasonable measures to identify the chief executive officer of an entity, or the person who performs that function, for which you are unable to obtain or confirm the beneficial ownership information, and treat the entity as posing a high risk and apply special measures.
- Verify whether you monitor the entities you consider to pose a high risk more frequently than other entities, and apply special measures to mitigate the risks.

Third party transactions

To conduct this assessment, we may:

- Review your procedures, processes and controls for situations where you are not able to determine whether an account is to be used by, or on behalf of, a third party when there are reasonable grounds to suspect that it would be.

Politically exposed persons and heads of international organizations

To conduct this assessment, we may:

- Verify your records to confirm that you rate all your foreign politically exposed person clients as posing a high risk, as well as their family members and close associates.
- Review your records of domestic politically exposed persons and heads of international organizations, as well as those of their family members and close associates, to ensure that you have adequately assessed the level of risk posed by these clients. To do so, we look at a sample of

these clients to see if they meet the criteria you have established to rate a client as posing a high-risk.

- Verify whether you monitor your high-risk clients more frequently than your lower risk clients and apply special measures.
- Review transaction records involving politically exposed persons and heads of international organizations, as well as their family members and close associates, to confirm that you are reporting suspicious transactions when required.

Our focus

We will focus on the following:

- **Business relationships and ongoing monitoring:** we will focus on ensuring you have an adequate ongoing monitoring process in place.
- **Beneficial ownership:** we will focus on ensuring that you have a process in place to obtain, and take reasonable steps to confirm the accuracy of beneficial ownership information.
- **Third party determination:** we will focus on ensuring that you are taking reasonable steps to determine whether there is a third party to a transaction or giving instructions on an account.
- **Politically exposed persons and heads of international organizations:** we will focus on ensuring that you are taking reasonable steps to find out if your clients are politically exposed persons or heads of international organizations (including family members and close associates), and for those who pose a high risk, we will focus on the special measures you have in place.

3.3. Financial transactions reporting requirements

We use the methods described in this section to assess your compliance with financial transaction reporting requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents to meet the reporting requirements.
- Review your client records, transaction records and submitted reports to confirm that you adequately apply your policies and procedures.
- Interview your employees and agents to assess their knowledge of the reporting requirements.

Our focus

We will focus on confirming that you have sound policies, procedures, processes and controls in place to adequately meet the following requirements: to submit financial transaction reports to FINTRAC (when required); to submit the reports on time; and to submit complete and accurate reports.

3.3.1. Requirements related to all reports types (all report types)

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with reporting requirements. The methods apply to all report types (Large Cash Transaction Reports, Large Virtual Currency Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports, and Suspicious Transaction Reports), with the exception of Terrorist Property Reports, for which only the assessment method titled "All report types 5" applies.

We use comparison testing, follow-up testing, quality testing, and timing testing.

Comparison testing

(All report types 1) Reviewing changes in your reporting behaviour

We review your reporting history to identify important variations, such as a noticeable increase or decrease in reporting, and confirm that you send reportable transactions when required. If we observe changes, we check to see if we have an explanation for them on file. If not, we follow up with you. We may review your transaction records to see if there are reports that should have been sent to us.

Follow-up testing

(All report types 2) Ensuring that you resubmit the reports FINTRAC rejected for technical errors

FINTRAC can reject a report if it contains technical errors, such as the way the report is formatted, or when quality issues are identified by our validation process. At the assessment, we provide you with a list of rejected reports which you did not correct and resubmit.

If you think this list is incorrect, we may ask you to provide us with the FINTRAC generated External Report Reference Number or the Reporting Entity's Report Reference Number to allow us to further enquire. Refer to our guidance on Batch Reporting Instructions and Specifications and FINTRAC Web Reporting system (FWR, formerly F2R).

For the reports that were not resubmitted, we may ask you why that was the case. We may also look at the records of transactions to confirm whether they were reportable.

(All report types 3) Ensuring past reporting issues have been fixed

We review your records and transaction records to confirm that you have fixed previous compliance issues related to reporting, such as those identified by way of a voluntary self-declaration of non-compliance, and those identified through previous compliance assessment activities that FINTRAC has conducted.

Quality testing

(All report types 4) Ensuring you report on transactions handled by your agents

We verify that you are reporting the transactions conducted by your agents on your behalf. You, not your agents, are ultimately responsible for submitting these reports. We may ask you to give us a list of your agents, including agency agreements, and a list of the transactions conducted by each agent to ensure that reportable transactions were submitted to FINTRAC.

(All report types 5) Ensuring your reports are complete and accurate

We review the information in your reports to verify that they are complete and accurate.

When we assess the quality of your reports, we verify whether any information is missing, inadequate or incomplete. For example, if the address field in a report was blank, we would consider this to be missing information. If the field included a post office box rather than a civic address, we would consider this to be inadequate information. If the field showed a civic address without the city, we would consider this to be incomplete. All of the fields in your reports must be complete and accurate.

We review the quality of your reports by considering all of the fields, including those that are mandatory, mandatory if applicable, and reasonable measures fields.

When reasonable measure fields are left blank, we will examine your records to see if you had the information at the time of the transaction. If you did have the information but did not include it in the report, as required, we will ask you to explain why.

We assess the information reported in Part G, "Description of Suspicious Activity" of Suspicious Transaction Reports to verify that there is an adequate description of the reasonable grounds to suspect that the reported transaction(s), or attempted transaction(s), were related to the commission, or attempted commission, of a money laundering offence or a terrorist activity financing offence.

In Terrorist Property Reports, we verify that information about the property and the persons or groups that own or control it, and information about transactions or attempted transactions related to the property, has been provided.

(All report types 6) Ensuring that your third party service provider reports correctly

When you use a third-party service provider to submit reports on your behalf, we verify that the reports list the correct identification information, such as your business name, phone number and location, not the identification information of the service provider.

We examine your records of transactions to identify the ones that should have been reported, and then verify that the service provider sent us the reports with the correct identification information. If we cannot find the reports in our database under the name of your business, we will seek to determine if your service provider used the wrong identification information when it sent the reports to FINTRAC or if the reports were not submitted.

Timing testing

(All report types 7) Ensuring that you are sending reports on time

We assess whether you are submitting reports within the timelines set out in the PCMLTFA and associated Regulations, and as described in FINTRAC

guidance. We may review the reports you submitted and compare them to your transaction records to confirm that the reports were sent on time.

3.3.2. Large Cash Transaction Reports (LCTRs)

We use methods described in this section to assess your compliance with requirements relating to Large Cash Transaction Reports.

(LCTR 1) Confirming you are submitting LCTRs
(Applicable to all business sectors)

We ask you to provide us with a list of your cash transactions or records of transactions of $10,000 or more, or both, including transaction and client identification information, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Large Cash Transaction Reports you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your large cash transactions, one that comes directly from your business records or the systems that you or your third-party service provider may have used to gather the information to submit Large Cash Transaction Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be deposit slips, invoices, sales receipts, receipt books, foreign currency exchange transaction tickets, pit logs (casino sector), records of player buy-ins (casino sector), etc.

(LCTR 2) Confirming you are correctly applying the 24-hour rule to LCTRs
(Applicable to all business sectors)

We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat cash transactions of less than $10,000 conducted by, or on behalf of, the same person or entity, that, when combined, total $10,000 or more within a 24-hour period. We confirm that you combine these transactions and send us the

required Large Cash Transaction Reports when the transactions were made within 24 consecutive hours.

We also verify that you send us separate Large Cash Transaction Reports for lump-sum cash transactions of $10,000 or more, and that you do not combine these with cash transactions of less than $10,000 conducted within a 24-hour period.

(LCTR 3) Confirming that you are submitting all the required reports for a given transaction

(Applicable to financial entities, casinos and money services businesses)

We review your records to verify that you have submitted a Large Cash Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in cash from, or on behalf of, the same person or entity, in a lump sum or over a 24-hour period, for the purpose of initiating an outgoing international electronic funds transfer of $10,000 or more. We look at your transaction records or the Large Cash Transaction Reports in which you indicated that the disposition of funds was through an "outgoing electronic funds transfer". We may ask you to provide the report numbers for the Electronic Funds Transfer Reports and the Large Cash Transaction Reports to confirm that both types of reports were submitted to FINTRAC.

(LCTR 4) Reviewing exceptions to submitting LCTRs

Exception—Alternative to large cash transactions

(Applicable to financial entities)

If a financial entity has used the alternative to submitting Large Cash Transaction Reports, as permitted under the PCMLTFA and associated Regulations and as described in our guidance, we verify that all of the conditions associated with this exception were respected. We confirm that you submitted, within the prescribed timeframe, a complete and accurate Financial Entity Business Client Report that includes a list of all the clients to which the exception has been applied. If you continue to apply the alternative to a client who no longer meets the prescribed conditions, we will review the client's cash transactions to determine whether Large Cash Transaction Reports should have been submitted to FINTRAC.

Exception—Cash received from financial entities or public bodies or from a person who is acting on behalf of a client that is a financial entity or public body

(Applicable to all business sectors)

If you did not send us Large Cash Transaction Reports for clients who are financial entities, public bodies, or a person who is acting on behalf of a client that is financial entity or public body as the law permits, we will verify that the clients are financial entities or public bodies as defined in the PCMLTFA and associated Regulations. If they do not meet the definition, we may review the client's cash transaction history to determine if there are Large Cash Transaction Reports that should have been submitted to FINTRAC.

3.3.3. Large Virtual Currency Transaction Reports (LVCTRs)

We use the methods described in this section to assess your compliance with the requirements relating to Large Virtual Currency Transaction Reports.

(LVCTR 1) Confirming you are submitting LVCTRs

(Applicable to all business sectors)

We ask you to provide us with a list of your virtual currency transactions or records of virtual currency transactions of $10,000 or more, or both, including transaction and client identification information, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Large Virtual Currency Transaction Reports you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your large virtual currency transactions, one that comes directly from your business records or the systems that you or your third-party service provider may have used to gather the information to submit Large Virtual Currency Transaction Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be virtual currency exchange transaction tickets, deposit slips, invoices, sales receipts, receipt books, foreign currency exchange transaction tickets, pit logs (casino sector), records of player buy-ins (casino sector), etc.

(LVCTR 2) Confirming you are correctly applying the 24-hour rule to LVCTRs

(Applicable to all business sectors)

We review your policies and procedures, records of transactions, internal records and reports, and other documents to identify how you treat virtual currency transactions that total $10,000 or more within 24 consecutive hours, and that are conducted by, or on behalf of, the same person or entity, or when the amounts are for the same beneficiary. We confirm that you combine these

virtual currency transactions and send us the required Large Virtual Currency Transaction Reports when the transactions were made within 24 consecutive hours.

(LVCTR 3) Confirming that you are submitting all the required reports for a given transaction

(Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We review your records to verify that you have submitted a Large Virtual Currency Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in virtual currency, in a deemed single transaction, for the purpose of initiating an outgoing international electronic funds transfer of $10,000 or more. We look at your transaction records or the Large Virtual Currency Transaction Reports in which you indicated that the disposition of funds was an “outgoing international electronic funds transfer”. We may ask you to provide the relevant report numbers to confirm that both types of reports were submitted to FINTRAC.

3.3.4. International Electronic Funds Transfer Reports (EFTRs)

(Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We use methods described in this section to assess your compliance with the requirements relating to Electronic Funds Transfer Reports.

(EFTR 1) Confirming that you are submitting EFTRs

We ask you to provide us with a list of your international electronic funds transfers of $10,000 or more, including transaction and client information, when you are the initiator or final receiver of the international electronic funds transfer, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Electronic Funds Transfer Reports that you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your international electronic funds transfer transactions, one that comes directly from your business records or the systems you or your third-party service provider may have used to submit Electronic Fund Transfer Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be transfer slips, wire logs, foreign currency exchange transaction tickets, invoices, etc.

(EFTR 2) Confirming that you are applying the 24-hour rule to EFTRs

We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat international electronic funds transfers of less than $10,000 conducted by, or on behalf of, the same person or entity, that, when combined, total $10,000 or more within a 24-hour period. We then confirm that you combine these transactions and send us the required Electronic Funds Transfer Reports.

We verify that you send us separate Electronic Funds Transfer Reports for lump-sum international transfers of $10,000 or more, and that you do not combine these with international electronic funds transfers of less than $10,000 conducted within a 24-hour period.

We also verify that you do not combine incoming international electronic funds transfers with outgoing international electronic funds transfers. In addition, for outgoing international electronic funds transfers, we verify that you combine transactions correctly when applying the 24-hour rule for transactions conducted by, or on behalf of, the same client. We also ensure you correctly combine incoming international electronic funds transfers.

(EFTR 3) Confirming that you are submitting all the required reports for a given transaction

(Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We review your records to verify that you have submitted a Large Cash Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in cash, in a deemed single transaction, for the purpose of initiating an outgoing international electronic funds transfers of $10,000 or more. We look at your transaction records or the Large Cash Transaction Reports in which you have indicated that the disposition of funds was an “outgoing electronic funds transfer”. We may ask you to provide the relevant report numbers to confirm that both types of reports were submitted to FINTRAC.

Assessment methods LCTR 3, LVCTR 3 and EFTR 3 are identical and are repeated for ease of reference.

3.3.5. Casino Disbursement Reports (CDRs)

(Applicable to casinos)

We use the methods described in this section to assess your compliance with the requirements related to Casino Disbursement Reports.

(CDR 1) Confirming that you are submitting CDRs

For this test, we ask you to provide us with a list of your casino disbursement records of $10,000 or more, including transaction and client information, so we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reason behind this discrepancy.

To be clear, we do not require a list of the Casino Disbursement Reports that you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your cash disbursements, one that comes directly from your business records or systems. We may ask you to send us a sample of this list before requesting the complete list, in order to verify that it is in the format we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide records of the disbursements. These could be cheque registers, player tracking sheets, transaction logs, etc.

(CDR 2) Confirming that you are applying the 24-hour rule to CDRs

We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat disbursements of less than $10,000 received by, or on behalf of, the same client, that, when combined total $10,000 or more, within a 24-hour period. We confirm that you combine these transactions and send us the required Casino Disbursement Reports.

We also confirm that you send us separate Casino Disbursement Reports for lump-sum disbursements of $10,000 or more and that you do not combine these with disbursements of less than $10,000 conducted within a 24-hour period.

3.3.6. Suspicious Transaction Reports (STR)

(Applicable to all business sectors, with the exception of STR 13, STR 14 and STR 15)

We use the methods described in this section to assess your compliance with Suspicious Transaction Report requirements.

Suspicious Transaction Reports are of significant intelligence value to FINTRAC as they are the cornerstone of the Centre's mandate to detect, deter and prevent money laundering and terrorist activity financing. Suspicious Transaction Reports, and other reports, enable the Centre to conduct analysis and produce actionable financial intelligence, which it discloses to police, law enforcement and national security agencies when prescribed thresholds are met.

Most of the assessment methods described in this section are based on money laundering and terrorist activity financing indicators published in FINTRAC guidance and other well-known reliable sources, such as the Financial Action Task Force (FATF).

The assessment methods for Suspicious Transaction Reports serve to evaluate how you address suspicious transactions, as well as other requirements. We use them to:

- Assess your compliance with other requirements, such as the risk assessment, special measures, and ongoing monitoring requirements;
- Verify that you identify money laundering and terrorist activity financing indicators, as well as transactions that may give rise to reasonable grounds to suspect that the transactions, or attempted transactions, are related to the commission or attempted commission of a money laundering offence or terrorist activity financing offence;
- Verify that you have a sound escalation and decision-making process for suspicious transactions;
- Verify that all relevant business areas receive key information regarding suspicious transaction activity; and

- Verify that you are sending us Suspicious Transaction Reports when required.

When assessing the information we gather through the application of these methods, we will use the approach described in Part 1 to arrive at our conclusions. We will evaluate the body of information and the totality of the circumstances and take a holistic and reasonable approach when arriving at our conclusions.

We use monitoring and unusual transactions testing, testing of high-risk areas, money laundering and terrorist activity financing indicator testing, external information testing, comparison testing, transaction reversal and relationship termination testing, and business sector specific testing.

The methods described in this section apply to both completed and attempted suspicious transactions. Assessment methods relating to the quality and timing of reports can be found in section 3.3.1 (all reports types).

Monitoring and unusual transaction testing (STRs)

In this section, the words “alerts” and “unusual transactions” refer to completed or attempted transactions that have been identified or flagged as part of your internal monitoring process because they may be related to money laundering or terrorist activity financing. Alerts and unusual transactions should be further assessed in keeping with your policies and procedures and could eventually lead to a Suspicious Transaction Report.

(STR 1) Reviewing your policies and procedures on how you monitor activities and transactions

We review your policies and procedures to confirm that you have a monitoring process that enables you to detect, assess and, when required, report suspicious transactions related to money laundering and terrorist activity financing. If you use generic policies and procedures developed by an industry group or consultant, we verify that you have adapted these policies and procedures to your business, including monitoring procedures.

We may ask questions such as:

- Is your monitoring process automated, manual or both?

- How are you alerted to, or informed of, unusual transactions, and how do you prioritize and action these?
- When you receive an alert, what process do you follow to identify, assess, and make a decision about the unusual transaction and, when required, report the transaction to FINTRAC?
- How often do you review your transaction monitoring process to make sure it remains in line with your risk assessment, and policies and procedures?

(STR 2) Reviewing your monitoring rules

We review the automated and manual monitoring rules that you have put in place to confirm that they help you detect unusual transactions and provide alerts on potentially suspicious transactions. When we review your rules, we confirm that they are reasonable, put into practice, and that they monitor transactions in keeping with your risk assessment. We may also ask you how often you adjust the rules, what would cause you to adjust them, what steps you take to do so, and how you document these adjustments. We may verify whether you periodically review your rules, to confirm that you are not overlooking potentially suspicious transactions.

(STR 3) Reviewing unusual transactions

We review the unusual transactions identified by your monitoring system that you did not report to confirm that your decisions were sound.

We look into whether you use a risk-based approach to identify unusual transactions and generate alerts, so that you can direct more of your time and effort to areas of higher risks of money laundering and terrorist activity financing. For example, you may place more importance on transactions that present two or more money laundering or terrorist activity financing indicators.

If you do use a risk-based approach to manage unusual transactions, we will determine if your approach is reasonable. To do this, we will assess:

- If you have sufficient resources to monitor and review transactions based on the size of your business and its transaction volume.

- If you have a reasonable rationale to support the thresholds placed on the monitoring rules and unusual transactions.
- How often you monitor and action unusual transactions that pose a lower risk.

Testing high-risk areas (STR)

(STR 4) Reviewing your high-risk areas

We review client records and transaction records related to the high-risk areas identified in your risk assessment, such as high-risk clients, high-risk delivery channels, or high-risk jurisdictions. We may also review a sample of client records and transaction records for areas you did not determine to pose a high risk to ensure no gaps exist in your risk assessment or reporting procedures.

Money laundering and terrorist activity financing indicator testing (STR)

(STR 5) Identifying indicators consistently

We ensure that you are applying your money laundering or terrorist activity financing indicators in a consistent manner when submitting Suspicious Transaction Reports. We first review Part G of the reports you have submitted to identify the most common indicators listed. We then verify your records to assess whether you continue to submit suspicious transaction reports when these common indicators are present in other transactions, and there are reasonable grounds to suspect that the transactions are potentially related to money laundering or terrorist activity financing. If we identify suspicious transactions that were not reported, we will prioritize transactions that would have given FINTRAC new information for analysis.

(STR 6) Reviewing transactions for money laundering and terrorist activity financing indicators

As part of our risk assessment of your business, we identify money laundering and terrorist activity financing indicators that you may come across in the course of your business. We verify that these indicators inform your compliance program and support your efforts to detect, assess, and report suspicious transactions. Should we detect transactions that reflect these indicators in our

review of your client records and transaction records, we will look into the actions you took to determine whether they were reasonable.

In addition, while we recognize that you may prioritize certain indicators over others, we verify that your processes and systems do not overlook suspicious behaviour.

External information testing (STR)

(STR 7) Reviewing how you use publicly available information

We look at how you use publicly available information as part of your risk assessment, monitoring and Suspicious Transaction Report processes. Publicly available information includes news releases issued by industry regulators, police and other law enforcement agencies, mainstream news media, and other credible sources. We assess whether you take reasonable steps when you discover something of interest about a client. We will enquire about your reasons for not acting upon publicly available information.

(STR 8) Reviewing how you process information from credible sources

We verify how you use information received from police, law enforcement and national security agencies, and regulatory or supervisory bodies, related to money laundering and terrorist activity financing, to inform your compliance program. This information could include production orders, comfort letters, alerts and internal referrals. Specifically, we look at how you use this information to identify potential high-risk clients, take measures to reduce the risk related to these clients, and submit Suspicious Transaction Reports when required. We verify that the information is forwarded to your compliance officer or your compliance department when it is addressed to a different person or department.

FINTRAC will not ask to see sealed production orders nor those that include an order of non-disclosure.

Comparison testing (STR)

(STR 9) Verifying variances in actual versus expected transactional behaviour

We verify whether you detect when a client's transactions differ noticeably from what is expected and that you take action. We may review the client records and transaction records of clients whose transactions noticeably differ from those of similar clients. For example, a client may conduct more transactions or transactions of higher value than what is expected when compared to a group of similar clients.

(STR 10) Detecting unusual patterns

We review your client records of transactions for unusual patterns or connections that we determine meet the reasonable grounds to suspect threshold and should be reported. For example, we may look for:

- Clients who appear unrelated but have the same address or phone numbers.
- Clients who are in school or unemployed and conducting high-value transactions.
- People without any apparent relation making deposits into the same account.

When we search for patterns or connections, we look through your electronic or paper records, as well as through the reports you sent us. We also ask if you look for such patterns or connections and how you do so.

Transaction reversal and relationship termination testing (STR)

(STR 11) Reviewing your refunds, cancellations and overpayments

We review records of transactions where a refund cheque was issued because a customer returned an item, cancelled a life insurance policy, terminated a service, cancelled a real estate transaction, or overpaid for transactions. These situations may represent common money laundering and terrorist activity financing indicators, and as such, we review your procedures to ensure that you

are adequately assessing these situations and taking the necessary measures, as applicable.

(STR 12) Reviewing how you end relationships with clients and agents

The PCMLTFA and associated Regulations do not require you to end business relationships. That decision remains yours to make. However, if you decide to end a relationship with a client or an agent because of concerns related to money laundering or terrorist activity financing, we verify that you continue to monitor their transactions for possible suspicious transactions, and take steps to mitigate risks, until the relationship is officially ended.

Business-sector-specific testing (STR)

The Suspicious Transaction Report assessment methods described above are applicable to most business sectors. However, some sectors have characteristics that require specific testing.

(STR 13) Real estate: Reviewing how you use market values and local market conditions

(Applicable to real estate)

We verify that you detect purchase or sale transactions that are noticeably below or above the expected market value, based on local market conditions, to determine whether the transaction is suspicious. Real estate values and market conditions vary across Canada based on location, the economic cycle and other factors. We assess whether you are aware of these market conditions and that you identify transactions that are well outside their expected or average market value.

(STR 14) Real estate: Reviewing deals with last-minute changes in ownership

(Applicable to real estate)

We review transaction records, including client records, receipt of funds records, bank drafts and third party determination records where there are unexplained or last minute substitutions of the buyer. We assess whether you have identified these cases as needing further review and assessment for possible layering or hiding of the true ownership, or that the original purchaser may be instructed by a third party until the property is assigned.

(STR 15) Casino: Reviewing your issued cheques for unusual buy-ins or disbursements

(Applicable to casinos)

We review the cheques you issued to clients to identify unusual buy-ins or disbursements that may indicate an attempt to layer proceeds of crime. We first ask you to explain how you identify unusual buy-ins or disbursements, reduce potential risks, monitor the transactions, and decide whether to submit a Suspicious Transaction Report.

Then, we may ask you for a list of the clients you have issued cheques to, so that we can identify irregularities, such as clients who may have received more cheques than what would usually be seen. If we do identify irregularities, we ask for the client history information and look for suspicious buy-ins or disbursements that should have been reported.

3.3.7 Terrorist Property Report (TPRs)

We use the methods described in this section to assess your compliance with Terrorist Property Report requirements.

(TPR 1) Reviewing your correspondence with authorities
(Applicable as indicated below)

We review:

- For all business sectors, correspondence with the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS) in which you indicated that you are in possession or in control of property owned or controlled by, or on behalf of, a terrorist, terrorist group, or listed person.
- The reports that financial entities, life insurance companies, and securities dealers are required to submit under the Criminal Code or the Regulations Implementing the United Nations Resolution on the Suppression of Terrorism. These reports are sent to provincial or federal regulators, in which the business indicated being in possession or control of property owned or controlled by, or on behalf of, a listed entity or listed person.

If you have disclosed that you are in possession of such property, we confirm that you sent us a Terrorist Property Report. We also verify that the information in the Terrorist Property Report is consistent with the information you sent the RCMP, CSIS, and your regulator (if applicable).

(TPR 2) Verifying lists for terrorist or terrorist groups and listed persons
(Applicable to all business sectors)

We confirm the steps you take to determine whether your business possesses or controls the property of a terrorist, terrorist group or listed person, and submit a Terrorist Property Report. If you are, or were, in possession or control of such property, we verify that you sent us a Terrorist Property Report.

We may assess how you handle situations where you cannot determine, based on the information you have, if you are dealing with a terrorist, terrorist group or listed person.

Whether you cannot file a Terrorist Property Report because you cannot make the necessary determination, or whether you are able to file a Terrorist Property Report, we verify that you send us Suspicious Transaction Reports when required. The added information in the Suspicious Transaction Report may prove valuable to FINTRAC in its intelligence work.

We may compare your clients' names against the list published in the Regulations Establishing a List of Entities issued under the Criminal Code and the list published in the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. If one of your clients is on either list, we verify that you submitted a Terrorist Property Report.

3.4. Record keeping requirements

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with record keeping requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the record keeping requirements.
- Review your client records and records of transactions to confirm that you put these policies and procedures into practice.
- Verify that you keep records as required by the PCMLTFA and associated Regulations when reviewing your client records and transaction records.
- Records may include the following, as applicable:
  - account opening records;
  - credit card account and transaction records;
  - prepaid payment product account and transaction records;
  - records of large cash transactions or large virtual currency transactions
  - records of electronic funds transfer or virtual currency transfer transactions;
  - records of casino disbursements;
  - foreign currency exchange or virtual currency exchange transaction tickets;
  - information records;
  - records that you are required to keep under client identification and know your client requirements; and
  - copies of reports submitted to FINTRAC

- Verify that you keep the information that is required (for example, name, address, date of transaction, etc.) for each type of record. The information that you are required to keep is determined by the type of record that needs to be kept.
- Verify that your records are kept in a format that can be produced within 30 calendar days of a request, and confirm that you keep the records for five years, or as long as required by the PCMLTFA and associated Regulations.
- Interview your employees and agents to assess their knowledge of record keeping requirements.

Our focus

While we assess record keeping, we will focus on ensuring that you accurately record information that identifies persons and entities that open or control accounts, and conduct or direct transactions.

3.5. Correspondent banking relationship requirements

(Applicable to financial entities)

We use the methods described in this section to assess your compliance with correspondent banking relationships requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Review your records, including records of transactions to confirm that your policies and procedures are put into practice.
- Review your records of transactions to confirm that you, as applicable:
    - take all required measures as per the PCMLTFA and associated Regulations—described in FINTRAC guidance;
    - do not deal with a shell bank;
    - obtain the required approvals;
    - identify your clients, when required;
    - obtain and keep records of required information;
    - risk assess the relationship;
    - take special measures, when required; and
    - meet the requirements within the prescribed timeframes.
- Interview your employees and agents to assess their knowledge of correspondent banking requirements.

When we evaluate your risk assessment, we may:

- Verify whether you have considered correspondent banking relationship risks such as the correspondent bank's location, corporate structure, profile and reputation, clientele, products and services, type and volume of activity, openness to sharing information as needed, and regulatory history.

- Review your record of the correspondent bank's anticipated account activity, including products or services. We may ask if, and how, you use this information to review the transactions conducted through your correspondent banking accounts in order to determine whether there are transactions or attempted transactions that deviate from the terms of your agreement. We may also review the records of transactions to this end.

If your policies and procedures allow for:

  - Payable-through accounts: we verify that you take reasonable measures to confirm that the correspondent bank identifies its clients who have direct access to your correspondent banking services in a manner that is consistent with Canadian client identification requirements and that it has agreed to provide you with relevant client identification data upon request;
  - Nested accounts: as a best practice, we may review the information that you have about the downstream bank and the controls you have implemented to mitigate risk and monitor the transactions conducted by the downstream banks and their clients.

If your policies and procedures prohibit payable-through accounts and nested accounts, we will ensure you have the appropriate controls in place to detect transactions involving these types of accounts and, if detected, that you have taken remedial action in keeping with your policies and procedures.

As part of our assessment, we may also:

- Verify that you update information regarding your correspondent banking relationship, the type of information that you update, and how often you update it.
- Verify that you have disclosed all your correspondent relationships to us, which may include a review of your records of transactions to confirm.
- Review your process to end a correspondent banking relationship because of money laundering or terrorist activity financing concerns.

Our focus

We will focus on the steps you take to ensure that senior management has approved your correspondent banking relationships and is aware of the risks involved.

We will also focus on the steps you take to ensure that you are not dealing with a shell bank. Shell banks operate outside the country where they are incorporated and licensed; they are not affiliated to a financial services group that is supervised in that country. Shell banks pose a serious risk to the Canadian anti-money laundering and anti-terrorism financing regime because of the difficulty that exists in ensuring regulatory oversight for requirements such as customer due diligence and risk mitigation measures.

3.6. Foreign branches, foreign subsidiaries and affiliates requirements

(Applicable to financial entities, securities dealers, and life insurance)

We use the methods described in this section to assess your compliance with requirements relating to foreign branches, foreign subsidiaries and affiliates.

Foreign branches and foreign subsidiaries

Information on requirements relating to foreign branches and foreign subsidiaries is available in our guidance.

To conduct this assessment, we may:

- Review the policies and procedures that you developed for your foreign branches and foreign subsidiaries to ensure that they are adequate, and reflect Canadian obligations when it comes to:
    - the establishment and implementation of a compliance program, including policies and procedures to evaluate the risk of money laundering and terrorist activity financing and risk mitigation measures when risk is considered high;
    - record keeping and retention; and
    - client identification.
- Confirm that the Board of Directors (if you have one) has approved these policies and procedures before they are put into practice.
- Review your client records and transaction records to confirm that your foreign branches and foreign subsidiaries apply these policies and procedures to the extent permitted by the laws of the country where the branch or subsidiary is located. If the policies and procedures conflict with local laws, we may ask you for the reason of the conflict and whether you have informed FINTRAC and your primary regulator of this issue, and have considered how you plan to mitigate any associated risks.
- Confirm how you ensure that your foreign branches and foreign subsidiaries are implementing the policies and procedures.

Domestic and foreign affiliates

Information on requirements relating to affiliates is available in our guidance.

To conduct this assessment, we may confirm that you have adequate policies and procedures in place to share information with your affiliates for the purpose of assessing the risk of money laundering and terrorist activity financing, and detecting and deterring such offences.

As part of our evaluation of your risk assessment, we may:

- Verify that you have assessed the risk of money laundering and terrorist activity financing for all of your foreign and domestic affiliates. This includes verifying that you have implemented measures to reduce risks should foreign affiliates be located in higher-risk countries.
- Ask you how you use information from affiliates about suspicious activities or transactions in your compliance program.

Our focus

We will focus on whether, as described, your foreign branches and foreign subsidiaries have policies and procedures in place and whether you have policies and procedures in place to share information with your affiliates.

3.7. Money services business (MSB), and Foreign money services business (FMSB) registration requirements

(Applicable to money services businesses and foreign money services businesses)

We use the methods described in this section to assess your compliance with money services business and foreign money services business registration requirements.

We verify that you keep registration information up to date, respond to clarification requests, renew your registration, and cancel your registration (if applicable).

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the requirements relating to money services business and foreign money services business registration.
- Review your client records and transaction records to confirm that the information provided to FINTRAC is accurate and that your policies and procedures are put into practice.
- Interview your employees and agents to assess their knowledge of the registration requirements.

Our focus

We will focus on ensuring that your registration information is accurate and up to date.

3.8. Ministerial directives' requirements

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with requirements relating to ministerial directives.

The instructions provided in each ministerial directive will vary and, as such, our assessment will focus on the essence of the directive.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the ministerial directive requirements.
- Verify that your policies and procedures clarify what ministerial directives are and where they can be found. We may also look to see whether your policies and procedures indicate how often you should check for new, updated or amended directives; who should be informed when a directive is applicable to your business; and what steps to take to make sure the directive is being followed.
- Review your client records and transaction records to confirm that you put the policies and procedures into practice.
- Verify that you have taken action when directives are applicable through our review of your client records and transaction records. These records may include:
    - the verification of the identity of a person or an entity;
    - the exercise of customer due diligence, including ascertaining the source of funds of a financial transaction, the purpose of a financial transaction or the beneficial ownership or control of an entity;
    - monitoring financial transaction for an account;
    - keeping records;
    - reporting financial transactions to FINTRAC; and
    - complying with other requirements of the PCMLTFA and associated Regulations.

- Interview your employees and agents to assess their knowledge of the requirements relating to ministerial directives.
- Verify that your business, including foreign branches and subsidiaries (if applicable), follows the directives.

When a foreign branch or foreign subsidiary cannot comply with a directive because it conflicts with local laws, we may:

- Review your records to verify that you obtained documents to confirm the conflict.
- Verify that you informed FINTRAC of the reasons for the conflict and, as applicable, the principal agency or body that supervises or regulates your business under federal or provincial law within a reasonable period.
- Ask about the measures you put in place to reduce the risks.

When you conduct business in a foreign jurisdiction or with a foreign entity named in a ministerial directive, we may:

- Verify that your risk assessment considers the parameters of the ministerial directive.
- Verify that you apply the processes that you have in place to manage high-risk transactions associated with ministerial directives, including monitoring the transactions more frequently, applying special measures, and submitting Suspicious Transaction Reports when required.

Our focus

We will focus on determining whether you are adequately implementing ministerial directives.