apaylo

APAYLO RESOURCE

The Compliance Readiness Resource

for Canadian Money Services Businesses (MSBs)

A resource to understand what Apaylo's compliance team evaluates when onboarding Money Services Businesses — and what most applicants get wrong.

SECTION 1

Introduction

The purpose of this resource is to clearly articulate what our Compliance team is assessing, why it matters, and how onboarding decisions are made when evaluating merchants - particularly Money Services Businesses (MSBs)—under the FINTRAC / PCMLTFA regulatory regime.

This is not a checklist document. It is a compliance readiness standard.

What this means for you:

If you're approaching this document looking for a box-ticking exercise, you're likely to be disappointed — and your onboarding application may not succeed. Apaylo's compliance review is calibrated to the same standard a FINTRAC examiner would apply. That means surface-level documentation, generic templates, and nominal appointments won't get you through.

The merchants who move through this process smoothly are those who have built compliance programs that genuinely reflect how their business operates, who have put real people in real roles, and who treat compliance as a living part of their business rather than a one-time paperwork task.

This resource walks through each component of what's being assessed, why it matters, and what failure looks like in practice — so you can come prepared.

SECTION 2

Why Compliance Matters

A strong AML/ATF compliance program is not just a **regulatory requirement**; it is a **key protection** for your business.

It helps prevent your services from being misused for fraud, money laundering, or other criminal activity, which can lead to account closures, loss of banking and PSP relationships, and regulatory scrutiny. A well- designed, risk- based program demonstrates to partners, regulators, and customers that your business takes its obligations seriously, reducing legal, financial, and reputational risk over the long term.

Let's break down what's actually at stake:

Reloadable & Controlled

Banks and payment service providers conduct their own due diligence on the businesses they serve. A weak AML program is one of the fastest ways to lose a banking relationship — and regaining one is extremely difficult once lost.

Your operating licence

FINTRAC has authority to impose Administrative Monetary Penalties (AMPs) reaching into the millions for serious or repeated violations, and to refer matters for criminal prosecution.

Your reputation

In financial services, your compliance posture is visible. Partners, customers, and counterparties notice. A well-designed program is increasingly a competitive differentiator, not just a cost of doing business.

The merchants who build genuinely compliant programs aren't just doing it to get through onboarding. They're protecting the business they've built.

SECTION 3

Regulatory Framework

Merchants onboarding are expected to comply with all applicable Canadian financial crime laws and guidance, including but not limited to:

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA),
- FINTRAC Guidance and Interpretation Notices,
- Canadian Sanctions Regulations, and
- Applicable privacy, record- keeping, and data protection laws.

Compliance onboarding is performed with FINTRAC examination standards in mind, not minimum merchant expectations.

What each of these means in practice:

PCMLTFA is Canada's primary AML/ATF legislation. It defines who is a Reporting Entity, what their obligations are, and what penalties apply for non-compliance. If you are an MSB, this Act governs you directly.

FINTRAC Guidance and Interpretation Notices are FINTRAC's own published documents explaining how to interpret and implement the PCMLTFA. These are not optional reading — your policies and procedures should reflect them.

Canadian Sanctions Regulations are administered through Global Affairs Canada and impose obligations around screening customers and transactions against designated lists. Sanctions lists are updated frequently, sometimes multiple times per week.

Privacy and record-keeping laws including PIPEDA govern how you handle, store, and retain customer data. Your compliance program must address these alongside your AML obligations.

Note: Privacy legislation is subject to change. Merchants should confirm the current applicable requirements, or reference both PIPEDA and its proposed successor.

Note on the standard: Apaylo's review is not calibrated to what the minimum acceptable program looks like. It is calibrated to what a FINTRAC examiner would conclude during an examination. That is the bar being applied.

SECTION 4

How Compliance Evaluates Merchants

What We Are Actually Looking For

During onboarding, Compliance is assessing the following core questions:

- Is the merchant correctly classified as an MSB under PCMLTFA?
- Does the merchant understand its AML/ATF obligations or merely rely on templates or vendors?
- Is the compliance program aligned with the merchant's actual business model, products, and risk exposure?
- Are risks identified, documented, and mitigated—or ignored?
- Is there evidence of governance, accountability, and senior management oversight?

Documentation that exists only to "satisfy onboarding" without operational substance will not be considered sufficient and therefore not onboarded.

Here's what each of these questions is really probing:

Correct MSB Classification

Your regulatory classification under the PCMLTFA determines your entire compliance obligation set. Misclassification — or failure to register all applicable MSB activities with FINTRAC — means your program is built on an incorrect foundation. The compliance team will cross-reference your stated activities, your FINTRAC registration, and your actual business model.

Genuine Understanding of Obligations

There's a meaningful difference between a business that has internalized its obligations and one that has purchased a template or hired a vendor to produce documentation. Apaylo's review is designed to surface that distinction. Can your compliance officer discuss your program in detail? Does your documentation reflect real operational decisions?

Program Aligned to Actual Business

Generic policies describing a hypothetical MSB are one of the most common reasons applications stall. Your program must describe your business: how funds move, where risks arise, and how controls apply at each step. The disconnect between documentation and reality is immediately apparent to a trained reviewer.

Risks Managed, Not Just Listed

A risk assessment that names risks without describing controls or residual risk ratings provides no meaningful assurance. Apaylo looks for evidence that risks are actively managed — that thresholds are set, monitoring is in place, and there's a clear escalation path when something goes wrong.

Real Governance and Accountability

Who owns compliance at your organization? Do they have budget, authority, and independence? Does senior management receive compliance reporting? These determine whether your program functions as designed or exists only on paper.

Documentation that exists only to satisfy onboarding — without operational substance — will not be considered sufficient and will prevent approval.

SECTION 5

Compliance Program Documentation – General Expectations

Documentation Depth, Coverage & Quality Standards

Compliance documentation is expected to demonstrate regulatory seriousness, operational accuracy, and risk awareness. The focus is not on document length, but on whether the compliance framework fully and accurately reflects the merchant's business model, risk exposure, and control environment.

In plain terms: a well-structured 40-page program that accurately describes your business will outperform a 200-page generic document every time.

Apaylo's compliance team is not counting pages or checking whether you've addressed every topic in the abstract. They're asking: does this program describe this business? Could a FINTRAC examiner walk through it and conclude that the company understands its risks and has controls designed to manage them?

That standard requires documentation that is specific, consistent, implementable, and current — not documentation that is lengthy, comprehensive-sounding, or written by a vendor who has never seen your actual operations.

SECTION 6

Documentation Must Comprehensively Cover, At a Minimum:

- The merchant's business activities and services, including how funds and value move through the business,
- The regulatory classification of the business under PCMLTFA,
- Clearly defined roles, responsibilities, and governance structures,
- Customer onboarding, due diligence, and offboarding processes,
- Transaction monitoring and reporting obligations,
- Sanctions, PEP/HIO, and adverse media controls,
- Record-keeping and data retention practices,
- Risk assessment methodology and mitigation strategies,
- Training, oversight, and escalation procedures, and
- Independent testing and continuous improvement mechanisms.

Here's what each of these questions is really probing:

Documentation Area	What Compliance Looks For
Business activities & fund flows	Clear description of all products, services, and how funds move in and out of the business
PCMLTFA regulatory classification	Explicit identification of which MSB activities the business conducts and why
Roles & governance structure	Named roles with defined responsibilities; reporting lines; senior management involvement

Documentation Area	What Compliance Looks For
Customer onboarding & CDD	Step-by-step processes for onboarding, ongoing monitoring, and offboarding customers
Transaction monitoring & reporting	Defined thresholds, monitoring rules, STR/LCTR/EFT reporting processes
Sanctions, PEP/HIO & adverse media	Screening procedures, frequency, list sources, escalation processes
Record-keeping & data retention	What records are kept, where, in what format, and for how long
Risk assessment methodology	How risks are identified, scored, mitigated, and reviewed over time
Training & escalation procedures	Training schedule, role-specific content, completion tracking, escalation paths
Independent review & improvement	Review schedule, scope, independence requirements, remediation tracking

SECTION 7

All Compliance Documentation Must Be:

- Business-specific and risk-based, reflecting actual operations,
- Internally consistent, with no contradictions across policies,
- Clearly structured and indexed for regulatory review,
- Version-controlled, approved by senior management, and review-dated, and
- Written in a manner that employees could reasonably follow and implement.

Generic or boilerplate documentation that does not reflect your actual business operations is unlikely to meet Apaylo's or FINTRAC's expectations and may prevent successful onboarding. Merchants are encouraged to ensure their policies accurately describe how their business identifies, assesses, and manages AML/ATF risks in practice.

A closer look at each standard:

Business-specific and risk-based. Every policy must reflect your actual operations. Generic language that could describe any MSB is a red flag. If your policies reference products you don't offer or customer types you don't serve, that inconsistency will be flagged immediately.

Internally consistent. If your onboarding policy says you verify identity within 3 days and your risk assessment assumes 1 day, that contradiction undermines both documents. Reviewers read policies together, not in isolation.

Version-controlled and governance-approved. Documents must carry version numbers, review dates, and senior management sign-off. Undated or unsigned policies cannot be relied upon as evidence of an effective program.

Operationally implementable. Could a new employee at your company actually follow these procedures? If not, they won't satisfy the standard — and more importantly, they won't protect your business.

SECTION 8

FINTRAC's Five Mandatory Compliance Components (Non-Negotiable)

Every MSB must demonstrate the ***existence, implementation, and effectiveness*** of the following five elements.

These components are non-negotiable. FINTRAC examines for all five during inspections. Missing any one of them is grounds for rejection of your application.

1. Designated Compliance Officer (CAMLO)

A formally appointed Compliance Officer with authority, independence, and accountability must oversee AML/ATF and sanctions compliance and act as the primary FINTRAC liaison. "Name-only" appointments are not acceptable.

What "name-only" means — and why it fails: A compliance officer who has been given a title but lacks budget authority, decision-making power, or actual involvement in the program will not satisfy this requirement. FINTRAC examiners ask detailed questions of CAMLOs directly. If yours can't speak to the program in detail, that's a material finding.

Your CAMLO should be able to walk through your risk assessment, explain your monitoring thresholds, and describe what happened the last time a suspicious transaction was flagged — from memory.

2. Written Compliance Program

Policies and procedures must be tailored to actual operations and cover AML/ATF controls, customer due diligence, monitoring, reporting, sanctions, governance, and prohibited activities. Policies must clearly assign responsibility and be approved by senior management.

Your written program must cover all of the areas listed in Section 6 of this resource, and every procedure described must correspond to something your business actually does. Responsibility for each control must be assigned to a named role — not "the compliance team" generically. Version control and review dating are required.

3. AML/ATF Training Program

A documented, role-specific training program must be provided at onboarding and at least annually, with evidence of completion and relevance to the business's risk profile.

Documentation of a training program is not the same as evidence of a training program. You must maintain completion records for every training session — who attended, when, what was covered, and what assessment was used to confirm understanding. Generic e learning modules that don't reference your specific products, customer types, or red flags are unlikely to satisfy this requirement.

4. Risk Assessment

A comprehensive risk assessment must identify inherent and residual risks, document mitigating controls, and be reviewed periodically and upon material business changes.

Your risk assessment is the intellectual core of your compliance program — it should drive everything else. A weak assessment that rates all risks as "medium" without justification, or that lists risks without linking them to specific controls, is one of the most common reasons applications are delayed or declined.

5. Independent Effectiveness Review

An independent review must be conducted at least every two years (and after material changes) to assess control effectiveness and document remediation actions.

The reviewer must be genuinely independent — not the person responsible for day-to-day compliance, and not someone who reports to that person. The review must assess control effectiveness, not just existence, and must result in documented findings and remediation actions. Internal auditors can satisfy this if they have genuine independence; otherwise an external firm is required.

SECTION 9

Common Compliance Failures That Delay or Prevent Approval

- Policies not aligned with actual operations,
- Missing or weak risk assessment,
- No empowered Compliance Officer,
- Outdated sanctions coverage,
- No evidence of training execution, or
- Over- reliance on vendors without oversight.

These aren't edge cases. They appear in the majority of incomplete applications. Here's what each one looks like in practice — and how to address it:

Policies Not Aligned with Actual Operations

The documentation describes a business that doesn't match what the merchant actually does — different products, different transaction flows, different customer types. This is immediately apparent to a trained reviewer and requires a full rewrite to remediate. Before submitting any documentation, map your compliance policies line-by-line against how your business actually operates.

Missing or Weak Risk Assessment

Either no formal risk assessment exists, or it exists as a minimally customized template — rating all risks as "medium" without justification, or failing to link risks to specific controls. Your risk assessment should be the first document written, not the last. It should drive everything else in your program.

No Empowered Compliance Officer

A title has been assigned but the individual has no real authority, no budget, no independence from business operations, and limited knowledge of the compliance program. Your CAMLO must be genuinely empowered — with real authority to refuse transactions, escalate concerns, and implement controls regardless of business impact.

Outdated Sanctions Coverage

Sanctions lists are updated frequently. Programs that reference outdated regimes or lack real-time screening infrastructure fail on a foundational control. Document your sanctions screening process specifically: which lists you screen against, how frequently they are updated, and what happens when a match is identified.

No Evidence of Training Execution

A training curriculum exists in the compliance manual, but there are no completion records, no attendance logs, and no assessments to demonstrate anyone actually received the training. Maintain records for every training session.

Over-Reliance on Vendors Without Oversight

Compliance functions have been outsourced to a third party, and the merchant has no meaningful oversight of what that vendor is doing. The regulatory obligation stays with you, not the vendor. Regardless of what tools or vendors you use, your compliance officer must maintain oversight of all outsourced functions and be able to speak to their operation in detail.

SECTION 10

Final Compliance Position

Compliance onboarding is an assessment of **readiness, maturity, and accountability.** Merchants are expected to invest adequate resources into building and maintaining a **living compliance framework,** not static documentation.

Apaylo's compliance team assesses each application on its own merits and may:

- Require remediation or enhancements,
- Impose conditions, and
- Decline onboarding where risks are unacceptable.

This document is provided for guidance purposes only and does not constitute legal advice.

What this means in practice:

If your review surfaces gaps, that's not necessarily a closed door. Apaylo's compliance team works with merchants to understand what's missing and what remediation is required. But the merchants who come prepared — who understand their obligations, have built their programs with genuine care for the risks they manage, and can demonstrate that their documentation reflects how they actually operate — are the ones who move through the process smoothly.

The goal isn't a perfect document. The goal is a defensible program — one that a FINTRAC examiner could walk through and conclude: "This business takes compliance seriously, and it shows."

SECTION 11

Compliance Resources & Reference Materials

FINTRAC, AML Program & Independent Review Support

The following resources are provided to assist merchants in understanding regulatory expectations and preparing a compliant Anti-Money Laundering (AML), Anti-Terrorist Financing (ATF), and sanctions compliance framework in accordance with Canadian regulatory requirements.

FINTRAC & Core Regulatory Sources

Resource
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
FINTRAC – Money Services Business (MSB) Registration
FINTRAC Guidance – Compliance Program Requirements
FINTRAC Guidance – Risk-Based Approach
FINTRAC Guidance – Suspicious Transaction Reporting
FINTRAC Administrative Monetary Penalties (AMPs)
Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)
Canadian Sanctions (Global Affairs Canada)

Independent AML Audit & Effectiveness Review Providers

(Non-exhaustive list of commonly accepted and qualified providers)

Merchants requiring an independent AML audit or effectiveness review may consider engaging one of the following firms, subject to independence and suitability requirements.

- PwC (PricewaterhouseCoopers)
- Deloitte
- KPMG
- Ernst & Young (EY)
- BDO / RSM
- Grant Thornton LLP
- Outliers Solutions
- The AML Shop
- AML Incubator (AMLI)*

Merchants remain responsible for ensuring auditor independence, appropriate scope, and compliance with FINTRAC expectations.

**Note: Merchants are not required to use AMLI (or any specific provider). Merchants are explicitly encouraged to choose any independent and qualified reviewer that meets regulatory expectations. The independence requirement under FINTRAC applies to the review engagement itself, not to whether a service provider has unrelated engagements with other entities in the ecosystem. AMLI operates as an independent compliance firm, and any effectiveness review would be conducted in accordance with independence and professional standards.*

SECTION 12

Conclusion

Apaylo's objective is to work with legitimately operating, compliant merchants and to support a safe and resilient Canadian payment ecosystem. We aim to provide clear information about regulatory expectations so merchants can better understand and strengthen their AML/ATF and sanctions controls. However, Apaylo does not provide legal, regulatory, or compliance advice and cannot design or maintain AML/ATF policies or programs on behalf of merchants.

Book a call with our payment experts

At Apaylo, we believe in providing personalized support to help meet your unique needs. Our team of experts are ready to assist you and show you the power of Apaylo's payment solutions.

Book a call →

SECTION 13

Transparency & Onboarding

Disclosure – Use of Compliance Service Providers

Apaylo engages qualified third-party compliance professionals to support elements of its AML, ATF, and sanctions compliance framework.

AML Incubator ("AMLI") is one of the compliance service providers used by Apaylo for advisory, compliance program development, and ongoing compliance support services.

This disclosure is provided for transparency purposes only. Merchants are not required to engage any specific provider and may select an independent compliance consultant or audit firm of their choosing, provided regulatory expectations, independence, and competency requirements are met.

onboarding decisions are based on the quality, completeness, and effectiveness of the merchant's compliance framework.

Regulatory Disclosure

Apaylo is registered as a Foreign Money Services Business (FMSB) with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC").

FINTRAC Registration Number: M22922184

Important Notice

These resources are provided for guidance and reference purposes only and do not constitute legal, regulatory, or compliance advice. Merchants remain responsible for ensuring ongoing compliance with all applicable laws, regulations, and regulatory guidance.