VOVE ID

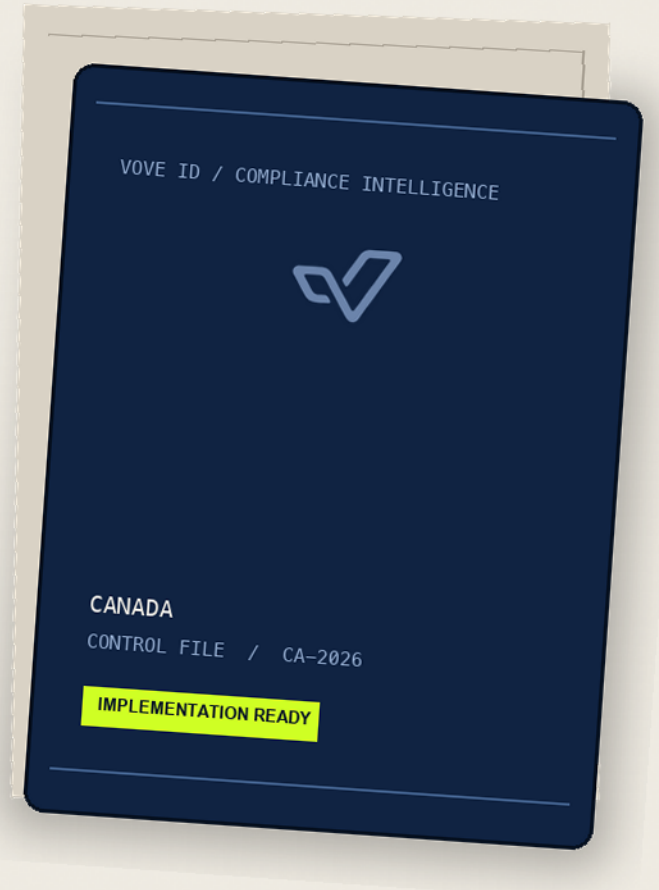
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

CANADA

CANADA / CA



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Canada KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for financial entities, money services businesses, payment service providers, securities dealers, virtual-currency businesses and other teams entering Canada. It separates federal AML, sanctions, corporate-transparency, privacy and retail-payments rules from sector-specific and provincial obligations; applicability must be resolved before any control is treated as mandatory.

Primary AML framework	**PCMLTFA and its regulations, with sector-specific reporting-entity duties**
Financial intelligence unit	**Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**
Suspicious transaction report	**No monetary threshold; submit as soon as practicable after reasonable grounds to suspect are established**
Large cash report	**CAD 10,000 or more, including qualifying 24-hour aggregation; file within 15 calendar days**
Large virtual-currency report	**CAD 10,000 equivalent or more, including qualifying 24-hour aggregation; file within 5 working days**
International EFT report	**CAD 10,000 or more for prescribed initiation or final-receipt roles; file within 5 business days**
AML beneficial ownership	**Individuals directly or indirectly owning or controlling at least 25%, plus ownership and control structure**
CBCA significant control	**25% voting rights or fair-market-value shares, or control in fact; federal corporations have register and filing duties**
Core AML retention	**Generally at least 5 years, but the event starting the clock varies by record**
MSB registration	**Canadian and qualifying foreign MSBs must register with FINTRAC before operating**
Retail payment providers	**In-scope PSPs must register with the Bank of Canada and meet operational-risk and safeguarding rules**
FATF public lists	**Canada was not named on the FATF public-list page reviewed 31 July 2026**

Scope and legal framework

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations form the core federal AML, CFT, sanctions-evasion reporting and record-keeping framework; The Criminal Code, United Nations Act, Special Economic Measures Act and program-specific regulations create separate terrorist-property and sanctions duties; The Canada Business Corporations Act creates an individuals-with-significant-control register and filing regime for federal corporations; The Personal Information Protection and Electronic Documents Act and substantially similar provincial laws govern private-sector personal information according to scope; The Retail Payment Activities Act and Regulations govern registration, operational risk and safeguarding for in-scope payment service providers; Provincial and territorial laws separately affect licensing, securities, consumer protection, corporate records and privacy

FATF context

Canada is a FATF member. As at 31 July 2026, it was not named on FATF's current public-list page for jurisdictions subject to increased monitoring or a call for action. FATF's Canada page records the mutual-evaluation and follow-up history; absence from a public list is not a finding that every control is fully effective.

IMPORTANT	This checklist is general regulatory information, not legal advice, a licence determination or a statement that every row applies to every Canadian business. It reflects primary and authoritative material reviewed on 31 July 2026. Confirm entity type, reporting-entity category, activity, customer, province or territory, incorporation jurisdiction, regulator, registration and licensing perimeter, live FINTRAC reporting instructions, sanctions regulations, privacy scope and later legal developments with qualified Canadian counsel and the competent authorities before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and licensing perimeter

Resolve the legal entity, activities, customers, delivery model and provincial nexus first. Federal AML registration or reporting status does not replace another federal or provincial authorization.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
PCMLTFA obligations apply to the persons and entities in section 5, with detailed duties that vary by reporting-entity category and activity.	Map each entity, product and flow to the applicable section 5 category and regulations before assigning controls.	Signed perimeter memorandum, activity map, reporting-entity classification, regulator mapping and legal conclusions.	PCMLTFA, ss. 5-6; FINTRAC, Who must report
Canadian MSBs and foreign MSBs that direct and provide prescribed services to persons or entities in Canada must register with FINTRAC before beginning covered operations.	Classify foreign exchange, remittance, money-order, crowdfunding and virtual-currency services; complete registration before launch and keep registration information current.	Service analysis, registration application, FINTRAC number, registry extract, renewal calendar and change filings.	PCMLTFA, ss. 11.1-11.2; FINTRAC, Money services businesses
An in-scope payment service provider must be registered with the Bank of Canada before performing retail payment activities, subject to the RPAA geographic test and exclusions.	Apply the five payment-function test, geographic scope and exclusions; obtain registration before launch and separately assess FINTRAC MSB status.	RPAA scope memo, registration decision, public-registry extract and AML registration reconciliation.	RPAA, ss. 2, 4-6 and 23; Bank of Canada, Criteria for registering PSPs
Provincial laws can separately regulate money services, securities, consumer contracts, privacy and corporate records.	Build a province-by-province matrix for every customer and operating nexus; document licences, registrations and exemptions before service begins.	Provincial matrix, regulator correspondence, licences, exemptions, counsel advice and renewal controls.	FINTRAC, MSB guidance; Bank of Canada, RPAA registration criteria

2. COMPLIANCE PROGRAM, GOVERNANCE AND RISK ASSESSMENT

Compliance program, governance and risk assessment

A reporting entity's program must be reasonably designed, risk-based and effective, not a generic policy pack detached from its Canadian activities.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Every reporting entity must establish and implement the prescribed compliance program and ensure it is reasonably designed, risk-based and effective.	Obtain senior approval for a program mapped to the entity's category, products, customers, channels, geography and sanctions-evasion exposure.	Approved program, legal mapping, board record, risk appetite, control inventory and accountable owners.	PCMLTFA, s. 9.6(1)-(2); PCMLTFR, s. 156
The program includes a compliance officer, written policies and procedures, documented risk assessment, ongoing training and an effectiveness review at least every two years.	Appoint an empowered officer, calendar training and independent testing, and track findings to verified closure.	Appointment, role charter, policy set, risk assessment, training logs, two-year review and remediation register.	PCMLTFR, s. 156; FINTRAC, Compliance program requirements
High-risk situations require prescribed special measures, including enhanced identification, relationship information and ongoing monitoring measures appropriate to the risk.	Define high-risk triggers and enhanced controls, approvals, review frequency and transaction monitoring; record the rationale for residual risk.	Risk methodology, high-risk file, enhanced checks, approvals, monitoring results and exception log.	PCMLTFA, s. 9.6(3); PCMLTFR, s. 157
Use of an agent, mandatary or service provider does not remove the reporting entity's responsibility; MSBs also have current duties to review agent eligibility and criminal records.	Perform pre-appointment and prescribed periodic agent checks, contract for compliance evidence, monitor performance and retain exit capability.	Eligibility review, criminal-record material, contract, agent list, oversight reports, issues and termination plan.	PCMLTFA, ss. 9.92-9.93; PCMLTFR, ss. 37.1 and 133; FINTRAC, MSB guidance

3. NATURAL-PERSON IDENTIFICATION AND VERIFICATION

Natural-person identification and verification

Identity triggers and permitted methods depend on the reporting-entity sector and transaction. Configure the precise rule, not a single universal onboarding threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
FINTRAC permits prescribed verification methods including government-issued photo identification, Canadian credit file, dual process, qualifying affiliate or member confirmation, and reliance arrangements.	Configure methods by sector and use case; retain required details showing the source was authentic or reliable, valid and current.	Method matrix, vendor configuration, source details, verification result, timestamps and quality tests.	PCMLTFR, ss. 105-109; FINTRAC, Methods to verify identity
Remote use of government-issued photo identification requires a process that authenticates the document and matches it to the person; collecting an image alone is insufficient.	Test document security, liveness or person match as appropriate, fraud signals, accessibility and manual escalation before accepting remote identity.	Authentication specification, vendor tests, decision logs, fraud review, exceptions and sampled files.	FINTRAC, Methods to verify identity, government-issued photo ID method
Identity must be verified at the prescribed sector and transaction triggers, including suspicious completed or attempted transactions regardless of amount where the rule applies.	Map every account, service and transaction trigger to timing, method and exceptions; route failed or incomplete verification to a controlled decision before proceeding.	Trigger matrix, workflow rules, attempted-transaction records, restrictions, closure decisions and STR assessment.	PCMLTFR, ss. 83-104 and 154; FINTRAC, When to verify identity
An agent or mandatary used for verification must operate under the prescribed written arrangement and provide the information needed for the reporting entity's records.	Execute a compliant agreement, validate the agent's method, retrieve evidence promptly and test the arrangement periodically.	Agreement, agent due diligence, method records, retrieval tests, sample reviews and corrective actions.	PCMLTFR, ss. 109 and 109.1; FINTRAC identity-method guidance

KYB, registries and beneficial ownership

Keep AML beneficial ownership under the PCMLTFR separate from a corporation's own ISC duties. Provincial entities also require their own registry analysis.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Entity verification uses prescribed sources to confirm existence and requires the reporting entity to record the relevant incorporation, registration or governing details.	Obtain current registry and constitutional material, verify status and authority, and identify persons authorized to bind or instruct for the entity.	Registry extract, constituting documents, business number, addresses, directors, signatory authority and verification log.	PCMLTFR, ss. 106-109; FINTRAC, Methods to verify identity
For a corporation, AML records include directors, individuals directly or indirectly owning or controlling at least 25% of shares, and information establishing ownership, control and structure; trusts and other entities have tailored tests.	Trace every ownership layer to natural persons, calculate direct and indirect interests, record control and trust parties, and document when nobody reaches 25%.	Ownership chart, calculations, director list, trust records, source documents, confirmation steps and approvals.	PCMLTFR, s. 138; FINTRAC, Beneficial ownership requirements
Beneficial-ownership accuracy must be reasonably confirmed initially and during ongoing monitoring; prescribed high-risk CBCA cases require consultation of public ISC information. A material discrepancy must be reported within 30 days unless resolved within that period.	Compare customer data with reliable records and the federal ISC registry when required; resolve the discrepancy within 30 days or submit the prescribed report and retain the acknowledgement.	Registry search, comparison record, discrepancy case, customer clarification, Schedule 7 report and receipt.	PCMLTFR, ss. 138(2)-(5), 138.1 and Schedule 7
Most CBCA corporations maintain an ISC register and file ISC information with Corporations Canada; significant control includes at least 25% of voting rights or fair-market-value shares and control in fact.	For a federal corporation, identify ISCs, update the register at least annually and within 15 days of known changes, and make the required event and annual filings.	ISC register, annual enquiry, shareholder responses, change log, filings, receipts and exemption record.	CBCA, ss. 2.1, 21.1 and 21.21; Corporations Canada, ISC filing guidance

PEPs, HIOs and enhanced due diligence

Canadian PEP and head-of-international-organization duties vary by sector, account, relationship and transaction. Family-member and close-associate scope must follow the precise rule.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial entities, securities dealers and casinos have prescribed account-related duties to determine PEP, HIO, family-member and specified close-associate status at opening, through periodic monitoring and when relevant facts are detected.	Screen at each legal trigger, capture relationship and office details, and route possible matches to trained adjudication.	Screening configuration, match evidence, periodic-monitoring log, relationship analysis and disposition.	PCMLTFR, ss. 121-123; FINTRAC, Account-based PEP and HIO guidance
Specified sectors have transaction-related PEP and HIO determinations for prescribed transactions of CAD 100,000 or more, including certain international EFT and virtual-currency events.	Configure the exact sector and transaction triggers, aggregation where required, determination steps and escalation.	Trigger rules, transaction sample, determination record, relationship data, approval and monitoring case.	PCMLTFR, ss. 121-123; FINTRAC, Account-based PEP and HIO guidance
A foreign PEP determination triggers prescribed source-of-funds and source-of-wealth measures, senior-management review and enhanced ongoing monitoring for account-based sectors.	Establish and corroborate wealth and funds, obtain the required senior decision, define enhanced scenarios and review the relationship at the prescribed cadence.	Wealth narrative, source documents, senior approval, enhanced-monitoring plan, alerts and periodic review.	PCMLTFR, ss. 121-123; FINTRAC, PEP and HIO guidance
Domestic PEP and HIO status requires a risk determination rather than an automatic prohibition; prescribed measures follow when the relationship is high risk.	Document the risk assessment and apply enhanced measures proportionately, without treating status alone as proof of criminality.	Risk decision, supporting factors, enhanced checks, approvals, monitoring and review record.	PCMLTFR, ss. 121-123; FINTRAC, PEP and HIO guidance

Monitoring, suspicious reporting and confidentiality

Suspicion reporting has no monetary threshold. Case records must show when reasonable grounds to suspect were established and why submission was timely.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A reporting entity submits an STR for a completed or attempted transaction when there are reasonable grounds to suspect a connection to money laundering, terrorist activity financing or sanctions evasion.	Monitor relevant activity, connect indicators to facts and context, and document the legal threshold for both filing and non-filing outcomes.	Scenario inventory, alerts, linked activity, investigation notes, decision rationale and STR receipt.	PCMLTFA, s. 7; Suspicious Transaction Reporting Regulations, s. 9; FINTRAC STR guidance
The STR is due as soon as practicable after completing the measures that enable the entity to establish reasonable grounds to suspect; there is no fixed monetary threshold or ordinary day count.	Timestamp detection, investigation and threshold decisions; prioritize submission and record a suitable explanation for any delay.	Case chronology, threshold approval, queue metrics, delay rationale, filing time and acknowledgement.	Suspicious Transaction Reporting Regulations, s. 9(2); FINTRAC, Reporting suspicious transactions
Subsequent suspicious transactions remain reportable while suspicion persists, and a threshold report does not replace an STR.	Link related cases and reports, reassess the customer periodically, and file every separately applicable cash, virtual-currency or EFT report.	Related-report references, customer reassessment, filing reconciliation and monitoring history.	FINTRAC, Reporting suspicious transactions, sections 7-8
A person must not disclose an STR or its contents with the intent to prejudice a criminal investigation.	Restrict STR access, prevent customer-facing tipping off, control legal and law-enforcement requests, and train staff on permitted handling.	Access list, audit logs, training, disclosure procedure, tested response and incident records.	PCMLTFA, s. 8; FINTRAC STR guidance

Cash, virtual currency, EFTs and the travel rule

Build separate reporting decisions for cash, virtual currency and international electronic funds transfers. Apply the current 24-hour aggregation mechanics and exceptions for each report type.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A reporting entity generally files an LCTR after receiving CAD 10,000 or more in cash in one transaction or qualifying aggregated transactions within a consecutive 24-hour window, subject to exceptions.	Aggregate by the prescribed conductor, third-party or beneficiary relationship, identify required parties and file within 15 calendar days after receipt.	Aggregation logic, LCTR, acknowledgement, identity and third-party records, exception and reconciliation.	PCMLTFR, ss. 126 and 132(3); FINTRAC LCTR and 24-hour-rule guidance
A reporting entity in scope generally files an LVCTR after receiving virtual currency worth CAD 10,000 or more in one transaction or qualifying 24-hour aggregation.	Apply the prescribed valuation, receipt and aggregation rules; capture wallet and transaction details and file within 5 working days.	Valuation source, wallet data, aggregation output, LVCTR, receipt, exceptions and quality review.	PCMLTFR, ss. 125, 126 and 132(4); FINTRAC LVCTR guidance
Prescribed financial entities, MSBs, foreign MSBs and casinos report initiation or final receipt of qualifying international EFTs of CAD 10,000 or more, including applicable 24-hour aggregation.	Determine the entity's role, cross-border character and aggregation; file within 5 business days after initiation or final receipt.	Funds-flow map, transaction data, aggregation test, EFTR, acknowledgement and filing reconciliation.	PCMLTFR, ss. 127-129 and 132(1); FINTRAC EFT guidance
The travel rule requires specified originator and beneficiary information to accompany prescribed EFT and virtual-currency transfers; recipients take reasonable measures when information is missing.	Configure mandatory message fields, preserve received information, hold or reject according to a documented risk-based policy, and test intermediaries and vendors.	Message specification, transfer samples, missing-data cases, disposition rationale, vendor tests and monitoring.	PCMLTFA, s. 9.5; PCMLTFR, ss. 124-124.1; FINTRAC travel-rule guidance

8. TARGETED FINANCIAL SANCTIONS AND LISTED PROPERTY

Targeted financial sanctions and listed property

Canada's sanctions programs are regulation-specific. The consolidated autonomous list is a useful screening aid but has no force of law and does not replace the operative schedules and prohibitions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Canadian persons and persons in Canada must comply with applicable prohibitions and dealing restrictions under the Criminal Code, United Nations Act, SEMA, JVCFOA and program-specific regulations.	Map products, persons, ownership, control, geography and activity to every applicable regulation and screen against current operative schedules.	Sanctions perimeter, regulation inventory, list versions, screening logs, ownership analysis and legal decisions.	United Nations Act; SEMA; JVCFOA; Global Affairs Canada, Current sanctions
The consolidated Canadian autonomous sanctions list is administrative and may lag amendments; the relevant regulation determines who is listed and what prohibition applies.	Use the consolidated list for detection but verify every potential match against the current regulation and schedule before disposition.	Screening hit, regulatory verification, identity evidence, disposition, approval and list-update testing.	Global Affairs Canada, Consolidated Canadian Autonomous Sanctions List
Where the statutory trigger is met, listed person or entity property must be reported to FINTRAC without delay, in addition to disclosures, freezes or other action required by the underlying law.	Freeze or restrict as the operative rule requires, escalate immediately, submit the FINTRAC property report and make every other required disclosure without tipping off.	Property record, freeze or restriction, legal analysis, FINTRAC report, authority disclosure and timestamps.	PCMLTFA, s. 7.1; FINTRAC, Reporting listed person or entity property
A completed or attempted transaction suspected to relate to sanctions evasion also requires an STR; a property report does not replace that assessment.	Run a separate reasonable-grounds-to-suspect assessment, file promptly when met and link related property and transaction reports.	Sanctions-evasion case, facts and indicators, STR decision, filings, cross-references and acknowledgement.	PCMLTFA, ss. 2 and 7; FINTRAC, Report suspected sanctions evasion

9. RECORDS, RETRIEVAL AND REGULATOR ACCESS

Records, retrieval and regulator access

Five years is common in the AML regulations, but the event that starts the clock depends on the record. Keep a record-level schedule rather than applying one deletion date to every file.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Records required by the PCMLTFR are generally retained for at least five years after the record-specific event, such as the transaction, account closure or last business transaction.	Map each record class to its exact trigger and legal hold; prevent early deletion and dispose securely when retention and other-law needs end.	Retention schedule, trigger mapping, system rules, legal holds, deletion certificates and sampled records.	PCMLTFR, s. 148; FINTRAC record-keeping guidance
Required records may be electronic if a paper copy can readily be produced and must be retrievable in the form and time required by FINTRAC.	Preserve authenticity, readability and linkages; test regulator retrieval across customers, accounts, transactions, reports and source evidence.	Data map, retrieval test, access logs, export sample, backup restore and issue remediation.	PCMLTFR, ss. 147-149
Beneficial-ownership records are kept for at least five years after the last business transaction, and STR-related records have their own prescribed retention requirements.	Create separate clocks for business relationships, beneficial ownership, transaction records and report copies; record the closure or last-transaction event.	Customer timeline, beneficial-owner record, STR copy, clock calculation and retention test.	PCMLTFR, ss. 138(5) and 148; Suspicious Transaction Reporting Regulations
Outsourcing storage or case management does not transfer accountability for complete, secure and prompt production.	Contract for Canadian legal requirements, access, export, preservation, incident notice and exit; exercise retrieval and migration periodically.	Vendor contract, data locations, access controls, retrieval exercise, incident test and exit package.	PCMLTFA, ss. 6 and 62; PCMLTFR, ss. 147-149

Privacy, biometrics and transfers

Resolve whether PIPEDA, a substantially similar provincial law, sector law or several regimes apply. AML retention authority does not authorize unrelated collection or indefinite reuse.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
PIPEDA requires accountability, identified purposes, appropriate consent where required, collection limitation, safeguards, access and retention controls for personal information in scope.	Map every KYC data element and purpose, identify legal authority and consent, minimize collection, control access and set defensible retention and deletion.	Data inventory, purpose and authority register, notices, consent record, access matrix, retention and privacy assessment.	PIPEDA, ss. 5-7 and Schedule 1; OPC, Privacy Guide for Businesses
Biometric templates and identity signals can be sensitive personal information; necessity, effectiveness, proportionality, consent and security must be assessed in the applicable jurisdiction.	Complete a privacy impact assessment before biometric use, document alternatives and bias testing, separate templates, limit reuse and provide deletion controls.	Privacy impact assessment, necessity test, consent flow, model tests, security design, vendor terms and deletion proof.	PIPEDA, ss. 5-7 and Schedule 1; OPC guidance on biometrics and sensitive information
Under PIPEDA, a breach posing a real risk of significant harm must be reported to the OPC and notified to affected individuals as soon as feasible; records of every safeguards breach are kept for 24 months.	Assess harm promptly, document the decision, report and notify when required, inform relevant third parties, and retain the complete breach record.	Incident chronology, harm assessment, OPC report, notices, third-party communications and 24-month record control.	PIPEDA, ss. 10.1-10.3; Breach of Security Safeguards Regulations, s. 6
An organization remains accountable for personal information transferred to a processor, including processing outside Canada, and must use contractual or other means to provide comparable protection.	Map locations and sub-processors, assess legal-access and security risk, contract for comparable safeguards, disclose cross-border practices and test deletion and return.	Transfer map, vendor assessment, contract, transparency notice, security review, audit and exit evidence.	PIPEDA Schedule 1, principles 4.1.3 and 4.8; OPC cross-border processing guidance

Payments, agents and practical evidence packs

Turn the legal perimeter into testable launch gates. Payment providers may simultaneously face RPAA, FINTRAC and provincial obligations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Since 8 September 2025, in-scope PSPs must maintain the prescribed operational-risk and incident-response framework and safeguard end-user funds when they hold them.	Implement the written frameworks, map systems and third parties, test incidents, reconcile safeguarded funds and obtain legal support for the safeguarding arrangement.	Frameworks, risk register, incident exercise, safeguarding legal analysis, daily reconciliation, exceptions and remediation.	RPAA, ss. 17-20; RPAR, ss. 5-17; Bank of Canada supervisory framework
Registered PSPs submit an annual report by 31 March following the reporting year and make other prescribed change, incident and new-activity reports.	Maintain a Bank of Canada obligations calendar, assign owners and reconcile every report to source data and registration information.	Calendar, annual report, source reconciliation, change notices, incident reports, acknowledgements and approvals.	RPAA, ss. 21 and 22; RPAR, ss. 18-20; Bank of Canada reporting guidance
A reporting entity remains responsible for activities performed through agents or service providers and must maintain evidence that delegated controls operate effectively.	Define responsibility, data and escalation in contracts; test onboarding, monitoring, reporting, privacy and sanctions controls end to end.	Responsibility matrix, contracts, control tests, case samples, service metrics, findings and verified remediation.	PCMLTFR, s. 133; RPAA, s. 87; Bank of Canada registration guidance
Each checklist row requires an explicit applicability decision, owner, current source and reconstructable operating evidence before launch.	Mark each row applicable, not applicable or pending legal confirmation; close blockers and obtain compliance, privacy, security and product approvals.	Completed checklist, applicability rationale, source snapshot, owner sign-off, test result, gap ticket and launch approval.	PCMLTFA, s. 9.6; PCMLTFR, s. 156; RPAA, ss. 17-20

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act
Justice Laws Website · Primary legislation
Open official source

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
Justice Laws Website · Primary regulation
Open official source

Suspicious Transaction Reporting Regulations
Justice Laws Website · Primary regulation
Open official source

FINTRAC obligations and guidance directory
FINTRAC · Official regulator guidance
Open official source

Compliance program requirements
FINTRAC · Official regulator guidance
Open official source

Methods to verify the identity of persons and entities
FINTRAC · Official regulator guidance
Open official source

When to verify identity - factors
FINTRAC · Official regulator guidance
Open official source

Beneficial ownership requirements
FINTRAC · Official regulator guidance
Open official source

PEP and HIO guidance for account-based sectors
FINTRAC · Official regulator guidance
Open official source

Reporting suspicious transactions
FINTRAC · Official regulator guidance
Open official source

Reporting large cash transactions
FINTRAC · Official regulator guidance
Open official source

Reporting large virtual currency transactions
FINTRAC · Official regulator guidance
Open official source

Reporting electronic funds transfers
FINTRAC · Official regulator guidance
Open official source

Reporting transactions under the 24-hour rule
FINTRAC · Official regulator guidance
Open official source

Travel rule for EFT and virtual-currency transfers
FINTRAC · Official regulator guidance
Open official source

Reporting listed person or entity property
FINTRAC · Official regulator guidance
Open official source

FINTRAC money services business guidance
FINTRAC · Official regulator guidance
Open official source

Money Services Business Registry
FINTRAC · Official register
Open official source

Canada Business Corporations Act
Justice Laws Website · Primary legislation
Open official source

Individuals with significant control
Corporations Canada · Official registry guidance
Open official source

ISC filing requirements
Corporations Canada · Official registry guidance
Open official source

United Nations Act
Justice Laws Website · Primary legislation
Open official source

Special Economic Measures Act
Justice Laws Website · Primary legislation
Open official source

Current sanctions imposed by Canada
Global Affairs Canada · Official government guidance
Open official source

Consolidated Canadian Autonomous Sanctions List
Global Affairs Canada · Official administrative screening list
Open official source

Personal Information Protection and Electronic Documents Act
Justice Laws Website · Primary legislation
Open official source

Breach of Security Safeguards Regulations
Justice Laws Website · Primary regulation
Open official source

Privacy Guide for Businesses
Office of the Privacy Commissioner of Canada · Official regulator guidance
Open official source

Privacy breaches at your business
Office of the Privacy Commissioner of Canada · Official regulator guidance
Open official source

Retail Payment Activities Act
Justice Laws Website · Primary legislation
Open official source

Retail Payment Activities Regulations
Justice Laws Website · Primary regulation
Open official source

Retail payments supervisory framework
Bank of Canada · Official regulator framework
Open official source

Criteria for registering payment service providers
Bank of Canada · Official regulator guidance
Open official source

FATF Canada country page
Financial Action Task Force · Official international assessment
Open official source

FATF black and grey lists
Financial Action Task Force · Official current-status source
Open official source

Document control

Version 1.1 / Published 31 July 2026 / Last reviewed 31 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice, a licence determination or a statement that every row applies to every Canadian business. It reflects primary and authoritative material reviewed on 31 July 2026. Confirm entity type, reporting-entity category, activity, customer, province or territory, incorporation jurisdiction, regulator, registration and licensing perimeter, live FINTRAC reporting instructions, sanctions regulations, privacy scope and later legal developments with qualified Canadian counsel and the competent authorities before launch.