KROTON Platform Compliance Report – FINTRAC Requirements Alignment

H3M Analytics Inc.

Finance Montréal, 4 Place Ville Marie Suite 300

Montréal, QC, Canada H3B 2E7

Executive Summary

FINTRAC's Mandate & Scope: The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit and AML/ATF regulator. FINTRAC administers the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its Regulations, ensuring that businesses implement measures to detect and prevent money laundering and terrorist financing . All "reporting entities" (financial institutions, securities dealers, money services businesses, casinos, real estate brokers, etc.) are subject to these laws. Key obligations under the PCMLTFA/Regulations include client due diligence ("Know Your Client"), client identification and beneficial ownership verification, comprehensive recordkeeping, determination of Politically Exposed Persons (PEPs) and third-party involvement, adopting a risk-based approach (RBA), ongoing monitoring of business relationships, and mandatory reporting of certain transactions (suspicious transactions, large cash transactions, electronic funds transfers, large virtual currency transactions) as well as screening/reporting related to sanctions and terrorist property. FINTRAC also requires every reporting entity to implement an internal compliance program (with policies, training, and independent effectiveness review) to ensure these obligations are met.

Purpose of this Report: This compliance report maps the FINTRAC requirements under the PCMLTFA and Regulations to the capabilities of the **KROTON** compliance platform. Each major compliance domain is analyzed in turn – from KYC and client identification rules through to reporting obligations and program governance. For each domain, we summarize the regulatory requirements (with references to the law and FINTRAC guidance) and describe how specific **H3M KROTON modules** support and fulfill those requirements. The KROTON software suite (e.g. **KYC Miner**, **Scenario Manager**, **Case Manager**, **Sanctions Miner**, **SWIFT Miner**, **RUMI Adverse Media Search**, and built-in dashboards/logs) provides an integrated solution that helps financial institutions remain compliant with FINTRAC's requirements. By digitizing client due diligence, automating transaction monitoring and reporting workflows, and maintaining robust audit trails, KROTON enables regulated entities to confidently meet their obligations under PCMLTFA/PCMLTFR. The following sections detail this alignment across all key compliance areas.

Compliance Area	Relevant Law / Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
KYC – Identification & Verification	PCMLTFA **s.6.1**; PCMLTFR (ID methods)	**KYC Miner; KYC 360° Dashboards**	Captures required ID data, verifies per prescribed methods, stores evidence with audit trail; keeps profiles current.
Client Identification & Beneficial Ownership	PCMLTFA **s.6.1**; PCMLTFR **s.138** (BO); FINTRAC BO guidance (≥25%)	**KYC Miner; KYC 360° Dashboards; RUMI – Adverse Media**	Records corporate structure & ≥25% BOs, supports registry/doc checks, adverse-media screening of principals.
Third-Party Determination	PCMLTFR **s.134**, **s.136**	**KYC Miner; Case Manager; KYC 360° Dashboards**	Forces third-party inquiry on onboarding/trigger events; records third-party details; ties to client and transaction records.
PEP & HIO Identification / EDD	PCMLTFA **s.9.3**; PCMLTFR (EDD measures)	**Sanctions Miner; KYC Miner; RUMI – Adverse Media**	Screens for foreign/domestic PEPs & HIOs; auto-flag high-risk, capture SoF/SoW and senior-approval; elevate ongoing monitoring.
Risk-Based Approach (RBA)	PCMLTFA **s.9.6(2)**; PCMLTFR **s.156(1)(c)**, **s.157** (special measures)	**KYC Miner; Scenario Manager; AI/ML Scoring; KYC 360°**	Configurable client/product/geography risk scoring; links risk tiers to tighter rules/thresholds and enhanced reviews.
Ongoing Monitoring (Business Relationships)	PCMLTFR **s.123.1**	**Scenario Manager; Case Manager; KYC 360° Dashboards**	Real-time monitoring with risk-calibrated scenarios; periodic KYC refresh & review tasks; full case audit trail.
Suspicious Transaction Reporting (STR)	PCMLTFA **s.7**; STR Regs (content & timing)	**Scenario Manager; Case Manager; Automated FIU Reports**	Detects red-flag patterns; guides RGS narrative; auto-populates/submits STR; retains report & supporting evidence.
Large Cash Transaction Reporting (LCTR)	PCMLTFR **s.126** (24-hour rule), **s.132(3)** (15-day timeline)	**Scenario Manager; Case Manager**	Detects single/aggregated cash ≥ $10k; pre-fills LCTR; tracks submission and retention.
Electronic Funds Transfer Reporting (EFTR) & Travel Rule	PCMLTFA **s.9.5**; PCMLTFR **s.124**, **s.127–128**, **s.132(1)**	**SWIFT Miner; Scenario Manager; Case Manager**	Parses SWIFT/wire data; validates originator/beneficiary fields; flags intl EFTs ≥ $10k; pre-fills EFTR and logs filing.
Virtual Currency – LVCTR & VC Travel Rule	PCMLTFR **s.124.1** (info w/ transfer), **s.132(2)** (LVCTR)	**Scenario Manager; Case Manager**	Monitors crypto inflows; aggregates ≥ $10k (24h); pre-fills LVCTR (asset, hash, wallets); captures sender/receiver data for travel rule.

Compliance Area	Relevant Law / Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Sanctions & Terrorist/Listed Property Reporting (TPR/LPEPR)	PCMLTFA **s.7.1** (+ Criminal Code s.83.1, UN Act, SEMA, Magnitsky)	**Sanctions Miner; Case Manager**	Daily list screening (UN/OSFI/etc.); blocks/freeze on true hits; generates TPR/LPEPR and logs immediate filing.
Recordkeeping & Retention	PCMLTFA **s.6**; PCMLTFR **s.144–146**	**Built-in Audit Logs; Data Warehouse; Director (Reporting)**	Retains copies of reports/records ≥ 5 years; immutable user/action logs; fast retrieval/export for exams.
Compliance Program & Biennial Effectiveness Review	PCMLTFA **s.9.6(1)–(3)**; PCMLTFR **s.156(1)(a–f)**, **s.156(3–4)**	**Director (Compliance Dashboard); Audit Logs; Scenario Manager; Case Manager**	Embeds policies via rules/workflows; program KPIs & evidence for audits; supports independent **2-year** effectiveness review & remediation tracking.
Training (staff, agents, foreign branches)	PCMLTFR **s.156(1)(e)**	**Director (Compliance Dashboard); Audit Logs**	Tracks usage/completion artifacts; surfaces gaps via metrics; evidences training as part of program review.

Know Your Client (KYC) Compliance

FINTRAC KYC Requirements: Under Canadian law, reporting entities must perform thorough due diligence to "know" their clients at onboarding and throughout the relationship. This starts with identifying each client and verifying their identity using government-issued ID or other FINTRAC-approved methods (as required by PCMLTFA Section 6.1 and detailed in regulations). In practice, KYC entails collecting all pertinent client information – full legal name, date of birth, address and contact details, occupation or business type, source of funds, purpose and intended nature of the account or relationship, etc. For entity clients, KYC includes understanding the ownership and control structure (see Beneficial Ownership below) and verifying the entity's existence (e.g. via corporate registries). FINTRAC expects that the information gathered is sufficiently detailed to create a comprehensive client profile, which should be kept accurate and up-to-date. This client profile forms the baseline for assessing whether a client's transactions are consistent with their declared profile and for detecting red flags. In short, **businesses must know who their clients are and the risk they pose** – failing which, accounts should not be opened (indeed, PCMLTFA prohibits opening an account if identity cannot be verified).

How KROTON Supports KYC: The **KROTON** platform centralizes and streamlines the KYC data collection and review process. The **KYC Miner** module allows institutions to digitally capture all required client information in configurable forms and checklists. It records identity document details, client background information, and relevant financial details. **KYC Miner** is designed for *flexible and precise customer risk evaluation*, meaning firms can customize the data fields and risk scoring models to align with their internal policies. For example, KROTON can automatically assign each client a risk rating (e.g. Low, Medium, High) based on factors like their occupation, net worth, transaction volumes, country of residence, etc. These risk scoring rules are defined by the institution to reflect FINTRAC's guidance on risk factors. The platform also supports attachments of KYC documents (scanned IDs, proof of address, corporate documents), with secure storage and audit trails. By having a 360° view of the client in one place, compliance officers can readily *"know their customer"* at a glance. KROTON's **KYC 360° Dashboards** display the client's profile data alongside risk indicators and any alerts/cases associated with that client, which provides a continuously updated picture. Moreover, if any client information needs periodic refresh (e.g. ID expired or annual income update), the system can flag it for review. In summary, **KROTON enhances KYC compliance** by ensuring all required client data is captured, risk-assessed, and easily accessible for ongoing due diligence.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Know Your Client (KYC)	• PCMLTFA s.6.1 (Identity verification) • FINTRAC Client Due Diligence Guidance (2021)	KYC Miner; KYC 360° Dashboards	Captures comprehensive client information and documents; assigns risk scores based on customizable factors; provides 360° client profile views so that the firm can easily monitor and update KYC data over time.

Client Identification & Beneficial Ownership Compliance

Regulatory Requirements: FINTRAC's rules set strict standards for client identification and beneficial ownership verification. **Identity Verification:** Every reporting entity must verify the identity of persons and entities when opening an account or conducting certain transactions (e.g. large cash or wire transfers) . Identification must be done using methods prescribed in the *PCMLTFR* (such as original government-issued photo ID, credit file checks, or dual-process combinations) and must be completed either face-to-face or via acceptable technology before certain transactions occur. The identity information to collect includes the client's full name, date of birth, address, and identification document particulars (type, number, issuing authority). For non-face-to-face onboarding, FINTRAC provides specific guidance (e.g. using credit bureau dual-source checks or reliable digital ID providers).

Beneficial Ownership: In the case of clients that are corporations or other organizations, the firm is required to obtain information on the *beneficial owners* – the individuals who ultimately own or control 25% or more of the entity . This means gathering the names of major shareholders (25%+ ownership), directors and senior management, as well as the structure of the company. The institution must also take *reasonable measures* to confirm the accuracy of this beneficial ownership information (for example, by reviewing official corporate registries or documentation) . Identifying beneficial owners is crucial because it "removes the anonymity of individuals behind corporate accounts" and helps detect front companies or shell entities. FINTRAC expects that if a client is an entity, the reporting entity will record all required ownership details and update them through ongoing monitoring. If beneficial ownership information cannot be obtained or verified, that itself is a red flag and may trigger refusal of service or an STR filing. In summary, **the law mandates knowing who you are dealing with – not just the person fronting the transaction, but any underlying principals.**

KROTON Platform Support: The **KYC Miner** module in KROTON directly addresses client identification and beneficial ownership requirements. During client onboarding workflows, KYC Miner enforces mandatory collection of identification data: it will not allow an account to be approved until all key fields (name, DOB, ID type/number, etc.) are entered and verified by a compliance user. The platform's **RUMI – Adverse Media** integration can also help here by screening the names of beneficial owners for negative news or sanctions hits (ensuring that hidden principals are vetted). Once the beneficial owners and directors are recorded, KROTON can automatically cross-check them against sanctions and PEP lists (via **Sanctions Miner**, see later section) as an added compliance step. The **audit log** features of KROTON maintain evidence that ID was verified on a certain date by a specific employee, which is crucial for demonstrating compliance to regulators. In essence, **KROTON ensures that no client is onboarded without proper identification and that the ultimate owners of entity clients are documented and verified,** thereby fulfilling FINTRAC's KYC and beneficial ownership obligations.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Client Identification & Beneficial Ownership	• PCMLTFA s.6.1 (Verify identity per regulations) • PCMLTFR Part 1 – ID Methods & Beneficial Ownership (25% threshold) • FINTRAC Guidance: Confirming Beneficial Owners	KYC Miner; KYC 360° Dashboards	Enforces collection of all required ID details for individuals (with audit trail of verification); records corporate client ownership structures and ≥25% beneficial owners; supports document upload and registry checks to confirm ownership information, flagging any gaps before onboarding.

Recordkeeping & Retention Compliance

Regulatory Requirements: Canadian AML regulations impose comprehensive recordkeeping obligations on reporting entities.

Records to Keep: For each client and transaction, specific records must be created and retained. These include: client identification records (copies of IDs or reference numbers of verification documents), account opening records (such as signature cards or account agreements), transaction records for certain types of transactions, and copies of all reports submitted to FINTRAC . For example, if an institution receives a large cash amount (≥ $10,000), it must create a *Large Cash Transaction Record* capturing details like the date, amount, the payer's name, address, DOB, occupation and the purpose of the transaction . Similar detailed records are required for large virtual currency transactions and electronic funds transfers, as well as for any *receipt of funds* ≥ $3,000 (which triggers a "receipt of funds record" requirement) . Additionally, when a business relationship is established, a record of the *purpose and intended nature* of the relationship must be kept (this often forms part of the KYC record).

Retention Period: FINTRAC mandates that all such records be retained for *at least five (5) years* from their creation or the event in question. For instance, a copy of every Suspicious Transaction Report (STR) or Terrorist Property Report filed must be kept for 5 years after it was submitted . Account-specific records are generally kept for 5 years after an account is closed, and identification records 5 years after the last transaction. The law also requires that records be kept in a manner that they can be provided to regulators within 30 days upon request (indicating they should be well-organized and accessible). In summary, **robust recordkeeping is a cornerstone of compliance** – without the required records, an institution cannot demonstrate it met its obligations.

KROTON Platform Support: The **KROTON** compliance platform inherently functions as a secure digital repository for all client and compliance records. **KYC Miner** and related modules store client profiles, including copies of identification documents and data points collected (these serve as the electronic *client ID record*). Every transaction alert or case in **Scenario Manager** or **Case Manager** automatically logs the relevant transaction details, which contributes to required records (e.g. an alert generated for a large cash deposit will contain fields for amount, date, account, etc., satisfying the large cash transaction record requirements if properly configured). KROTON also provides standardized templates and forms that map to regulatory record needs – for example, when filing a Large Cash Transaction Report via the system, a PDF copy of that report is saved, meeting the requirement to keep a copy. **Built-in Audit Logs** ensure that every user action (data entry, approval, report submission) is time-stamped and immutable. This means an auditor can retrieve, say, the exact STR report filed on a certain date along with who filed it, or the exact client information record at onboarding. KROTON's data retention settings are aligned to the 5-year rule by default, ensuring that records are not purged prematurely. In fact, data can be retained longer or archived as needed for legal holds. The **search and export** functions allow quick retrieval of records by client, account, or date – addressing the requirement to produce records to FINTRAC examiners within 30 days. By using KROTON as the central system of record, an institution significantly reduces the risk of missing or misplacing required documentation. **In essence, every required record – from KYC details to transaction reports – is captured and stored in KROTON's database with an auditable history, ensuring full compliance with recordkeeping and retention obligations.**

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Recordkeeping & Retention	• PCMLTFA s.6 (Keep records per regulations) • FINTRAC Record Keeping Guidance – 5 Year	KYC Miner; Scenario Manager; Case	Automatically logs and stores all client data, transaction details, and compliance reports in a secure database. Every alert and case file

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
	Retention • PCMLTFR Part 1 – Required Records (transactions, reports, etc.)	Manager; Built-in Audit Logs	serves as a digital record (with time-stamps and user stamps). All records are retained ≥5 years by default, and can be quickly retrieved or exported to satisfy audits and regulator requests.

Politically Exposed Persons (PEP), HIO, and Third Party Determination Compliance

Regulatory Requirements – PEP/HIO: The PCMLTFA and its regulations require financial institutions to determine whether clients (or beneficial owners of clients) are *Politically Exposed Persons* (PEPs) or *Heads of International Organizations* (HIOs) and to apply enhanced measures if so. A **PEP** generally refers to an individual who holds or has held a prominent public position, such as a head of state or government, high-ranking politician, senior government, judicial or military official, etc., either in a foreign country or domestically, as well as their immediate family members and close associates . An **HIO** is the head of an international organization (e.g. UN, IMF) or their close associates . The law (PCMLTFA s.9.3) mandates that in prescribed circumstances (typically at account opening for new clients, and during certain large transactions for non-account holders) the institution must make a PEP/HIO determination . If a client is identified as a *foreign PEP* or a *HIO*, the institution **must treat them as high-risk** and undertake specific Enhanced Due Diligence (EDD) measures . These measures, as set out in regulation, include obtaining senior management approval to keep or open the account, taking reasonable measures to establish the source of the client's funds or wealth, and conducting enhanced ongoing monitoring of that relationship. For *domestic PEPs* (Canadian PEPs) or HIOs, the same measures are required if the institution's risk assessment deems the person high risk . In all cases, the determination and the measures taken must be documented.

Regulatory Requirements – Third Party Determination: Separately, FINTRAC rules require taking reasonable measures to determine if a client is acting on behalf of a **third party** in certain scenarios (for example, when a large cash transaction or large virtual currency transaction is conducted, or when opening an account) . A third party in this context means anyone who instructs or directs the client to carry out the transaction – effectively the "beneficial actor" behind the scenes . The institution must ask the client if there is a third party involved and, if yes, record the third party's information (name, address, DOB for individuals, or business details for entities) . Even if no third party is identified, the fact that the determination was made (or if the institution suspects one but can't confirm, that must be noted) should be recorded. This requirement is aimed at unmasking situations where a client might be fronting for someone else (e.g. money mules, strawmen).

KROTON Platform Support: KROTON provides strong support for both PEP screening and third-party identification as part of its client due diligence workflow. Upon client onboarding or during periodic refresh, **KYC Miner** automatically checks the client's details against updated PEP lists. The platform maintains integrated watchlists (e.g. global PEP databases) within the **Sanctions Miner** module – this includes foreign PEPs, domestic PEPs, HIOs, and their known family members. If a new client matches a name on a PEP list (or if an existing client is later added to such a list), KROTON will flag it as a **PEP Hit** requiring review. Compliance analysts can then review the alert in **Case Manager**, where the system prompts for the required EDD steps – for example, a workflow checklist might require the analyst to input the source of funds information and to obtain a manager's approval in the case record. The **RUMI – Adverse Media** integration further complements this by searching the client's name in news sources for any derogatory information, which is especially useful for assessing source of wealth and any corruption red flags tied to PEPs. The platform's data model also has fields to tag a client as a PEP or HIO and to record details like the office held and the date of determination. This allows the institution to easily generate reports of all PEP clients and confirm that enhanced monitoring is in place (KROTON can automatically elevate the risk rating of PEP clients to High and trigger more frequent transaction reviews for them).

In summary, KROTON automates PEP/HIO screening at onboarding and ongoing monitoring, and enforces third-party inquiry and recordkeeping, with built-in workflows that guide staff to complete all enhanced due diligence actions required under the law.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
PEPs, HIOs & Third Party Determination	• PCMLTFA s.9.3 (PEP/HIO determination) • PCMLTFR Part 1 – EDD for PEPs (senior management approval, source of funds) • FINTRAC Third Party Determination Guidance	KYC Miner; Sanctions Miner; RUMI (Adverse Media); KYC 360° Dashboards	**PEP/HIO:** Automatically screens clients against PEP lists at onboarding and refresh; flags matches for enhanced due diligence (records source of funds, triggers management approval workflows, and marks client as high-risk for ongoing monitoring). **Third Party:** Built-in form fields and prompts to ask about third-party involvement on relevant transactions; requires input of third-party details if applicable, and logs this information as part of the client's records.

Risk-Based Approach (RBA) Compliance

Regulatory Requirements: Adopting a Risk-Based Approach is a fundamental principle of Canada's AML regime. Under PCMLTFA Section 9.6 and corresponding Regulations, every reporting entity must assess and document the risk of money laundering or terrorist financing in their activities . This **enterprise-level risk assessment** involves evaluating factors such as the types of clients you serve, the products and services you offer, delivery channels, and geographic locations of your business, to identify areas of high or low risk . The law specifically enumerates certain risk factors: client risk factors (e.g. PEPs, cash-intensive businesses), geographic risk factors (e.g. dealings in high-risk jurisdictions), product/service risk factors (e.g. private banking, correspondent banking), and other relevant factors . The institution must **document its risk assessment methodology and results** – essentially, produce a written analysis of where the highest risks lie and why. Importantly, if at any time a situation or client is determined to be high-risk, the law requires the institution to apply *"special measures"* or enhanced controls . These special measures may include increased monitoring, additional scrutiny on source of funds, senior management sign-off for high-risk clients or transactions, etc. The regulations also state that risk assessments must be kept up to date and re-evaluated when new products or technologies are introduced . In practice, FINTRAC expects that institutions will categorize their customers (and certain activities) by risk level and tailor their compliance efforts accordingly – more rigorous KYC and monitoring for higher risk, and vice versa. An effective RBA underpins compliance: it ensures that resources are focused where the risks are greatest.

KROTON Platform Support: KROTON is built to facilitate a risk-based compliance program. The **KYC Miner** module allows for custom risk scoring models: compliance teams can define risk scoring rules and weightings for various factors. For example, using KROTON's configuration, a firm can set points for certain client attributes (say, +10 points if the client's country is on a watchlist, +5 if the client is in a high-risk industry like gambling, +20 if the client is a PEP, etc.). KROTON then computes a risk score for each client and assigns a risk rating (Low/Med/High) dynamically. These ratings are visible on the **KYC 360° Dashboard** and can trigger different treatment: a *High Risk* tag on an account can automatically prompt the system to schedule more frequent **Ongoing Monitoring** reviews (in Scenario Manager) for that client's transactions. The platform also supports recording the institution's overall inherent risk assessment factors. In the admin settings, there are modules to document the enterprise risk assessment: users can input narratives about product risks, country risks, and mitigating controls. This essentially acts as a repository for the firm's official risk assessment documentation, which can be exported for regulators.

More directly, the **Scenario Manager** in KROTON lets institutions implement detection rules that correspond to their risk appetite. For instance, if the RBA identifies that electronic funds transfers to certain high-risk countries are a major risk, Scenario Manager can have a rule to specifically monitor and alert on those transactions above a low threshold. This ensures that high-risk scenarios (as defined by the risk assessment) are getting automatically flagged. KROTON's architecture thereby links the risk assessment to actual controls in place. Additionally, when new products or delivery channels are introduced (e.g. launching a new online platform), KROTON can be used to perform a *"change risk assessment"* – capturing what new risks might emerge and adjusting scenario rules accordingly. **In summary, KROTON operationalizes the Risk-Based Approach** by providing tools to quantify client risk, to document the institution's overall ML/TF risk assessment, and to calibrate monitoring and due diligence efforts in line with those risks. This demonstrably meets FINTRAC's expectations that compliance measures are commensurate with risk exposure.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Risk-Based Approach (RBA)	• PCMLTFA s.9.6(2) (Risk assessment policies) • PCMLTFR 156(1)(c) (Assess/document risk factors) • FINTRAC RBA	KYC Miner; Scenario Manager; KYC 360° Dashboards	Enables custom risk scoring of clients (assigns Low/Med/High risk ratings based on configurable criteria); centralizes documentation of enterprise risk assessments; ties risk

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
	Guidance – Enhanced measures for high risk		levels to control intensity (e.g. high-risk clients automatically receive more frequent monitoring through Scenario Manager rules).

Ongoing Monitoring & Business Relationships Compliance

Regulatory Requirements: Once a business relationship with a client is established (e.g. an account is opened or regular dealings are in place), reporting entities are required to conduct **ongoing monitoring** of that relationship (PCMLTFR Section 123.1) . Ongoing monitoring means scrutinizing client transactions and behavior over time to ensure they are consistent with the client's profile and to identify any suspicious activities. According to FINTRAC's guidance, ongoing monitoring involves several elements: (1) detecting any transactions that should be reported as suspicious; (2) keeping the client's identification information and beneficial ownership information up to date; (3) reassessing the client's risk level when necessary; and (4) checking that the client's transactions and activities match what you would expect given your knowledge of that client (their occupation, stated source of funds, risk category, etc.) . The frequency and intensity of ongoing monitoring must be *risk-based*: higher-risk clients should be monitored more frequently and with more scrutiny, whereas lower-risk clients can be reviewed on a periodic sample basis . If a client is categorized as *high risk*, FINTRAC requires **enhanced ongoing monitoring** – this could mean reviewing transactions monthly or even daily, setting lower thresholds for alerts, conducting more frequent refresh of KYC information, and requiring managerial approvals for certain activities . All steps taken in ongoing monitoring must be documented, and records of findings (like unusual activity detected and rationale for conclusions) should be kept . In essence, ongoing monitoring is the continuous extension of the initial due diligence throughout the life of the client relationship, ensuring that any anomaly or change in behavior is noticed and evaluated. The requirement *"to periodically conduct monitoring"* underscores that this is not a one-time event but an ongoing process integrated into daily operations.

KROTON Platform Support: KROTON was designed as a continuous monitoring system, perfectly aligning with FINTRAC's ongoing monitoring expectations. The heart of this is the **Scenario Manager**, which runs automated monitoring rules on transactions *in real time and on a scheduled basis*. Financial transactions (from core banking or trading systems) stream into KROTON, where Scenario Manager evaluates them against various detection rules (scenarios). These scenarios encapsulate patterns of potential concern – for example, large cash deposits, rapid movement of funds in and out, unusual activity for the client's profile, etc. If a scenario's conditions are met, an alert is generated. All alerts flow into **Case Manager**, which is used by compliance analysts to investigate and document the outcome. This continuous alert generation and investigation cycle *is* ongoing monitoring in practice: KROTON is always watching the client's transactions against risk indicators. The system also keeps the client's risk profile in mind – scenarios can be tuned to a client's risk rating (for instance, require tighter thresholds for high-risk clients).

Additionally, KROTON's **KYC 360° Dashboards** assist in the periodic review aspect of ongoing monitoring. A compliance officer can pull up a dashboard for a high-risk client and see an overview of all their recent transactions, any alerts or cases in the last period, changes in their profile (e.g. updated address or employer), and so forth. The dashboard can highlight if certain KYC information is out-of-date, prompting the officer to refresh those details. KROTON can schedule periodic review tasks: for example, it can create a workflow every 12 months for medium-risk clients and every 3 months for high-risk clients, reminding the team to review the account activity and update any client info. During such reviews, analysts can log their observations and if needed escalate anything suspicious as an STR. Importantly, **all monitoring and review actions are logged** – the Case Manager will show a complete audit trail of what was reviewed, by whom, and what decisions were made . This evidences to regulators that ongoing monitoring is indeed being carried out consistently. KROTON's ability to aggregate transactions across accounts and time also helps identify patterns (e.g. the 24-hour rule aggregations, or structuring attempts over multiple days). In summary, **KROTON operationalizes ongoing monitoring** by providing continuous automated surveillance via Scenario Manager, and by facilitating structured periodic reviews via dashboards and cases – ensuring that any unusual client activity is detected, investigated, and, if necessary, reported in a timely manner, as required by FINTRAC.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Ongoing Monitoring & Business Relationships	• PCMLTFR s.123.1 (Periodic monitoring of business relationships) • FINTRAC Ongoing Monitoring Guidance – ensure transactions align with client profile • Enhanced Monitoring for High-Risk (EDD)	Scenario Manager; Case Manager; KYC 360° Dashboards	Continuously monitors all client transactions against risk-based rules (Scenario Manager alerts flag unusual or suspicious patterns in real time). Provides dashboards and automated tasks for regular account reviews, with special focus on high-risk clients (more frequent checks, detailed review logs). All monitoring activities and findings are documented in Case Manager, creating an audit trail of compliance oversight.

Suspicious Transaction Reporting (STR) Compliance

Regulatory Requirements: One of the most critical obligations under the PCMLTFA is the duty to report suspicious transactions. PCMLTFA Section 7 requires every reporting entity to *"report to FINTRAC every financial transaction that occurs or is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to a money laundering or terrorist financing offence."* In plain terms, if an institution **detects a transaction or attempted transaction that raises suspicions of ML/TF**, it must promptly file a Suspicious Transaction Report (STR) with FINTRAC. There is no monetary threshold for STRs – any amount can be suspicious – and the reporting must occur within 30 days of when the suspicion was first detected. The law and FINTRAC guidance emphasize the standard of *"reasonable grounds to suspect (RGS)"* as the trigger: this is a low threshold, meaning if a reasonable person in similar circumstances would suspect, an STR should be filed . Institutions are expected to have processes to identify red flags (unusual transaction patterns, inconsistencies with client profile, known typologies, etc.). The content of the STR must include all known details of the transaction, the parties involved, and a narrative explaining what is suspicious and giving the context (the “grounds for suspicion”). Not filing an STR on time, or at all, when required is a serious violation. FINTRAC also advises that organizations should keep records of STRs and should **not tip off** the client. Additionally, any related transactions that are connected to a suspicious transaction should also be reported (either in the same STR or a subsequent one, applying the 24-hour rule for multiple related suspicious transactions).

KROTON Platform Support: KROTON’s Scenario Manager and Case Manager are pivotal in ensuring suspicious activities are detected and reported. The platform comes with a library of pre-defined detection scenarios (rules) that correspond to common money laundering red flags – for example: sudden large cash deposits by a client with no known source of funds, multiple fund transfers to unrelated third parties shortly after account funding, rapid in-and-out movements (“turnover”) of funds, unusual geographic patterns (transactions to high-risk countries), etc. These scenarios can be tailored and new ones can be added based on the institution’s experience or emerging typologies. When any such rule triggers, Scenario Manager generates an alert which is then reviewed in **Case Manager**. Case Manager provides an investigation workspace: analysts see the transaction details, the client’s profile, and any related alerts. Crucially, KROTON has a built-in narrative builder and templates to guide analysts in recording the “Reasonable Grounds to Suspect” analysis. This ensures that by the time a determination is made, the analyst has documented why the activity is deemed suspicious (or not). If the conclusion is that the activity is indeed suspicious, KROTON can directly facilitate the filing of an STR. The system can auto-populate the FINTRAC STR form fields with information from the case (client details, transaction particulars, etc.), and the analyst need only fill in the narrative of suspicion (which they may have already drafted in Case notes). The STR can then be submitted electronically to FINTRAC through KROTON’s reporting interface, and a copy is stored for the records. By integrating alert handling with STR filing, **KROTON ensures no suspicious incident “falls through the cracks.”** Every alert must be dispositioned (e.g. “No suspicion – false positive” or “STR filed”) and this disposition is logged. Management dashboards in KROTON can show metrics such as number of STRs filed, pending suspicious cases, etc., which help in oversight. Additionally, if law enforcement or regulators later ask for the rationale behind an STR, the Case Manager contains the full investigation history supporting that report. Overall, **KROTON greatly strengthens STR compliance** by automating the detection of suspicious transactions and streamlining the investigation-to-reporting pipeline, ensuring timely and well-documented STR submissions to FINTRAC.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Suspicious Transaction Reporting (STR)	• PCMLTFA s.7 (Must report transactions with reasonable grounds to suspect ML/TF) • STR Regulations (SOR/2001-317) – STR content & 30-day timeline • FINTRAC Guidance	Scenario Manager; Case Manager	Scenario-based alerts flag suspicious patterns (potential ML/TF red flags) in real time. Case Manager aggregates all relevant transaction details and assists analysts in documenting their suspicion rationale (RGS narrative). If a transaction is deemed suspicious,

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
	on STR "reasonable grounds to suspect"		the system auto-generates a FINTRAC STR form with pre-filled data, allowing swift electronic filing. All STRs and their supporting case files are retained for 5+ years, demonstrating compliance in audits.

Large Cash Transaction Reporting (LCTR) Compliance

Regulatory Requirements: FINTRAC requires reporting of large cash transactions to deter the use of cash in illicit activity. A **Large Cash Transaction Report (LCTR)** must be submitted whenever an amount of cash **$10,000 or more** is received by a reporting entity in a single transaction . This applies to cash (coins and banknotes in any currency) but not to other instruments like cheques or bank drafts . In addition, the so-called "24-hour rule" aggregates multiple smaller cash amounts: if a reporting entity receives two or more cash amounts that total $10,000 or more *within 24 hours* (and they are either received from the same client, or by the same person, or on behalf of the same underlying party), that is treated as a large cash transaction and must also be reported . The LCTR must be submitted to FINTRAC **within 15 calendar days** of the transaction(s) . The content of the report includes detailed information about the transaction (date, amount, currency, how it was received), the person from whom cash was received (name, address, DOB, occupation) and, if applicable, the entity on whose behalf it was received, plus any account affected . Essentially, FINTRAC wants a complete picture of significant cash inflows. These reports help FINTRAC track potential money laundering via cash (e.g. structuring of deposits to avoid detection). It's worth noting that even if an armored car service delivers cash, the institution receiving it must still treat it as cash received from the client behind it . Failing to report a qualifying cash transaction or reporting late can result in penalties. Thus, processes must be in place to capture all cash transactions and check if they trigger reporting, including summing multiple transactions in a 24h window.

KROTON Platform Support: KROTON simplifies compliance with LCTR obligations by automating detection and documentation of large cash deposits. In the institution's transaction processing system (e.g. core banking), any cash deposit or withdrawal is flagged with a "cash" indicator that feeds into KROTON's **Scenario Manager**. KROTON has predefined scenarios to catch cash transactions ≥ $10,000 and to aggregate multiple cash transactions over 24 hours. For example, if a client makes three separate $4,000 cash deposits on the same day at different branches, Scenario Manager will sum these ($12,000 total) and trigger an alert for a reportable large cash event (applying the 24-hour rule). This alert then routes to **Case Manager** with all pertinent details (each deposit record, timestamps, teller IDs, etc.). KROTON's **Case Manager** can present a LCTR form template where much of the required info is auto-filled: the client's identity info (from KYC records), account numbers, each deposit amount and time, etc. The compliance officer just needs to verify the information, add any missing details (e.g. occupation if not on file, purpose of transaction if known), and then the report can be submitted to FINTRAC directly via the system's reporting interface. **SWIFT Miner** (for EFTs) isn't directly relevant for cash, but KROTON overall handles the data collation. Importantly, **KROTON ensures no reportable cash transaction is overlooked** – every cash entry above threshold generates an alert, and the workflow forces a decision: either file LCTR or mark why not (e.g. if it was exempt, though few exemptions exist for cash). After submission, KROTON keeps a copy of the LCTR and timestamps it, satisfying the recordkeeping requirement (the copy is kept for 5 years). The system can also produce management reports listing all LCTRs filed in a period, which helps the compliance team review for completeness. In summary, KROTON's monitoring and case management functionality acts as a safety net and an efficiency tool for large cash reporting, **automating aggregation, alerting, form population, and record retention for LCTRs**, so the institution remains consistently compliant with FINTRAC's cash reporting rules.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Large Cash Transaction Reporting (LCTR)	• PCMLTFR s. 126 & s.132(3) (Cash ≥ $10k and 24h aggregation rule) • FINTRAC LCTR Guideline – 15-day reporting timeline	Scenario Manager; Case Manager	Detects single or multiple cash transactions totaling ≥ $10,000 (24-hour aggregation) and automatically raises alerts. Case Manager pre-fills LCTR reports with client and transaction details, streamlining submission to FINTRAC. All such reports and underlying transaction records are saved with timestamps, ensuring timely filing and audit-ready documentation.

Electronic Funds Transfer Reporting (EFTR) Compliance

Regulatory Requirements: The law also mandates reporting of large electronic funds transfers. An **Electronic Funds Transfer Report (EFTR)** must be sent to FINTRAC when a reporting entity initiates or receives an international EFT of **$10,000 or more** in a single transaction, or multiple EFTs that total ≥ $10,000 within 24 hours, by or on behalf of the same person or entity . (Domestic EFTs within Canada are not reportable to FINTRAC under this requirement, only those that are outgoing from or incoming to Canada.) The EFTR must be submitted within 5 working days from the date of the transfer. Each EFTR includes information on the sender, the receiver, and the transaction (amount, date, financial institution info, etc.). In practice, banks satisfy this by capturing wire payment records – e.g. SWIFT messages – and populating the report. **"Travel Rule" information:** FINTRAC regulations (PCMLTFA s.9.5) also require that certain originator and beneficiary information *travel with the transfer* through the payment chain . This means the sending institution must include the sender's name, address and account number (or other identifier) with the wire message, and the receiving institution must take reasonable measures to ensure incoming wires have that info, and if not, take action (possibly report or refuse). The *PCMLTFR* provisions (e.g. s.127-128) detail what information must accompany an EFT. Failure to include required info or to report the EFT to FINTRAC can lead to compliance findings. In summary, institutions need systems to identify qualifying international EFTs, ensure the wire data fields are complete (not stripped of originator info), and to lodge the EFTR with FINTRAC in a timely manner.

KROTON Platform Support: KROTON covers EFTR obligations through its **SWIFT Miner** and scenario monitoring capabilities. **SWIFT Miner** module parses SWIFT payment messages (MT103, etc.) and other payment system logs to detect wires that meet the reporting criteria. It will flag any incoming or outgoing transaction ≥ $10,000 CAD (or equivalent) that is cross-border. The system checks if multiple smaller wires should be aggregated (similar to LCTR logic) for the same client in a 24-hour period. Once a reportable EFT is identified, an alert is generated in **Scenario Manager/Case Manager**. KROTON then assists the analyst in preparing the EFTR. It can extract all relevant fields from the wire (originator name, address, account, beneficiary details, amount, date, reference numbers) and present them in the electronic EFTR format. The **Sanctions Miner** integration also comes into play by screening the parties in the wire for sanctions or high-risk flags in real time, but regarding EFTR specifically, it ensures the data is captured. KROTON's workflow will highlight if any required originator/beneficiary information is missing from the payment message (for example, if an incoming wire lacks the originator address, the compliance team is alerted to that fact – which is a potential compliance issue or anomaly to follow up on). The platform can generate the EFTR and submit it through FINTRAC's system, logging the date of submission. The *travel rule* compliance is further enhanced by KROTON's rules that validate outgoing wire fields: before a SWIFT payment is sent, SWIFT Miner can be configured to validate that all mandatory originator information fields are populated, thus preventing defective messages. **In essence, KROTON automates the detection and reporting of large EFTs** by reading wire data, flagging reportable transfers, and auto-filling EFTR reports. By centralizing this in one system along with STR and LCTR processes, it gives compliance officers a unified view. They can be confident that every large international transfer is either reported or recorded with justification if not. This greatly reduces manual oversight needed and ensures compliance with both the reporting and "travel rule" aspects of the PCMLTFA for electronic funds transfers.

Compliance Area	**Relevant Law/Guideline**	**H3M / KROTON Module(s)**	**How the Platform Supports Compliance**
Electronic Funds Transfer Reporting (EFTR)	• PCMLTFA s.9.5 (Include originator info with EFT; ensure completeness) • PCMLTFR s.127-128 (Travel rule details) & s.132(1) (EFT 24h rule)• FINTRAC EFTR Guidance – ≥ $10k intl wires in or out reported within 5 days	SWIFT Miner; Scenario Manager; Case Manager	Monitors all wire transfers for cross-border transactions ≥ $10,000 (including aggregating multiple transfers in 24h) and raises alerts for reportable EFTs. SWIFT Miner parses wire messages to ensure required originator/beneficiary information is present; KROTON auto-populates EFTR reports with wire details for quick submission. Outgoing wires are validated for "travel rule" data, and any deficiencies or anomalies in incoming wires (missing info) are flagged for follow-up, thus maintaining full compliance with EFT reporting and information requirements.

Virtual Currency Transactions & LVCTR Compliance

Regulatory Requirements: As of June 2021, Canada extended "large transaction" reporting to **virtual currency (VC)** transactions. A **Large Virtual Currency Transaction Report (LVCTR)** must be filed when an amount equivalent to **$10,000 or more in virtual currency** (such as Bitcoin, Ethereum, etc.) is received by a reporting entity in a single transaction (or if multiple smaller amounts totalling ≥ $10k are received within 24 hours by/for the same person, analogous to the cash 24h rule) . This mirrors the large cash reporting requirement, but for cryptoassets. Notably, the trigger is receiving VC – for instance, if a money services business or other reporting entity receives $10k worth of cryptocurrency from a customer (perhaps in exchange for fiat or for a purchase), that event must be reported. The report must include the names and addresses of both transacting parties (if available), the type of virtual currency and amount, date, any crypto wallet addresses involved, transaction IDs (hash), and method by which the VC was received (e.g. in person, via wallet transfer, etc.). The required fields are specified by FINTRAC's form. Additionally, similar to wires, there is a **"VC travel rule"** now in regulation: when transferring virtual currency to another entity, certain identifying information about the sender and receiver should accompany the transfer (where technologically feasible) . If acting as an intermediary, one should ensure this info is passed along. The aim is to prevent anonymous crypto transfers exceeding the threshold. The LVCTR must be submitted within 15 days of the transaction (same as LCTR). With virtual currency's pseudo-anonymity, collecting information for the report can be challenging, but FINTRAC expects reporting entities to obtain whatever client details they can (client KYC info links to the crypto addresses).

KROTON Platform Support: KROTON has adapted to include virtual currency monitoring and reporting within its platform. Through its **Scenario Manager**, KROTON can monitor transactions involving cryptocurrency if the institution deals in VC. For example, if an exchange or bank integrates KROTON, any time a customer receives ≥ $10,000 worth of crypto (in one go or aggregated in 24h) into their hosted wallet or account, KROTON will trigger an alert for a reportable LVCT (Large Virtual Currency Transaction). The system can convert various cryptocurrencies to CAD in real time using exchange rates to determine if the $10k threshold is met. Once flagged, **Case Manager** guides the compliance analyst in compiling the LVCTR. KROTON's form for LVCTR includes fields for the **virtual currency type and amount**, the blockchain address or wallet ID, transaction hash, and the client's details. Much of this can be auto-filled from the transaction ledger and KYC records. The analyst would add any missing info (e.g. how the VC was received – a dropdown in the form). After verification, the LVCTR can be submitted directly to FINTRAC through the platform, and a copy is stored.

KROTON also helps with the **travel rule for virtual currency**: if the institution is sending a crypto transfer on behalf of a client, the system ensures that required originator and beneficiary information is attached. For instance, if sending Bitcoin, KROTON will log the beneficiary's name and crypto address and ensure the originator (client) details are recorded, so that if another reporting entity receives it, they have the info. If KROTON is used by both sender and receiver, this info flows naturally through the platform's records. **Sanctions Miner** is additionally configured to screen blockchain addresses against any known blacklists (since sanctioned or illicit addresses are sometimes published). By incorporating VC into its monitoring, **KROTON provides institutions with the same level of oversight on crypto transactions as on traditional funds**, which is crucial for compliance given FINTRAC's expanded rules. In short, any large crypto transaction will be caught by the system, reported within the deadline, and documented – satisfying the LVCTR requirements –

while the travel rule information is captured to accompany transfers, contributing to transparency in virtual asset movements.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Virtual Currency Transactions & LVCTR	• PCMLTFR s.124.1 (Include info with virtual currency transfer – travel rule)• PCMLTFR s.132(2) (Report receipt of VC ≥ $10k & 24h rule)• FINTRAC LVCTR Guidance – $10k crypto threshold, info required	Scenario Manager; Case Manager	Monitors cryptocurrency transactions in real-time, flagging any incoming virtual currency ≥ $10,000 (single or aggregated) for reporting. Case workflows populate the Large Virtual Currency Transaction Report with all necessary details (VC type, amount, wallet addresses, client info) for direct submission to FINTRAC. The system also captures required sender/recipient data for outgoing crypto transfers (fulfilling the “travel rule”), and integrates address screening to detect any high-risk crypto wallet identifiers, thereby extending compliance controls into the virtual asset domain.

Sanctions & Terrorist Property Reporting (TPR / LPEPR) Compliance

Regulatory Requirements: In addition to AML, Canadian institutions have obligations related to sanctions and terrorist property. While the Office of the Superintendent of Financial Institutions (OSFI) and Canadian law list prohibited parties (e.g. UN sanctions lists, terrorist entities under the Criminal Code, etc.), the PCMLTFA imposes a reporting duty via Section 7.1. Specifically, if a reporting entity **has in its possession or control property that it knows is owned or controlled by or on behalf of a terrorist or terrorist group, or a listed person (under Canadian sanctions regulations)**, it must report this to FINTRAC without delay . This is often referred to as a **Terrorist Property Report (TPR)** or **Listed Person/Entity Property Report (LPEPR)**. Essentially, upon a positive hit (e.g. an account belonging to a person on the UN 1267 terrorist list, or funds frozen due to sanctions), the institution must file a special report to FINTRAC, in addition to notifying regulators like OSFI and RCMP as required by other laws. Unlike STRs, TPRs are not about suspicion but about actual knowledge of listed property and must be filed *immediately* (ideally the same day the property is identified/frozen). The information in such reports includes details of the property (account, amount, type of asset), the listed person’s identity, and how and when it came under the institution’s control. Apart from this reporting, institutions are expected to have ongoing sanctions screening of customers and transactions (though that falls under OSFI guidelines, FINTRAC indirectly references it because failing to identify a listed person could lead to failing to report to FINTRAC). Therefore, ensuring up-to-date watch-list screening (UN, OSFI, etc.) is critical. In summary, if you have a **“listed person/property”**, freeze it and report it – and FINTRAC gets a report as part of that process.

KROTON Platform Support: KROTON includes robust sanctions screening and facilitates terrorist property reporting. The **Sanctions Miner** module performs automatic screening of client data against sanction lists (UN sanctions, OSFI's list of terrorist entities, Canadian government listed persons, as well as OFAC, EU lists if desired). This screening occurs at onboarding and regularly (e.g. daily refresh of lists and rescreening of the entire client base). If a client or counterparty match is found on any sanctions/terrorist list, Sanctions Miner generates an alert. KROTON will immediately flag the account and can even automatically block transactions through system integration, to prevent movement of funds. Such an alert flows into **Case Manager** for review. In the case manager workflow, if the hit is confirmed as a true match (not a false name similarity), the analyst will mark it as a positive hit. KROTON then provides a template for filing the Terrorist Property/Listed Person report. It collates all known details: the listed person's identifying info, details of the property (e.g. "Account #123456, Balance $50,000 frozen"), and references to the specific list/law under which the person is listed. The compliance officer can use KROTON to send the required report to FINTRAC immediately, and KROTON logs the date/time of filing. This ensures the **TPR/LPEPR is dispatched rapidly** in line with regulations.

Additionally, KROTON's integrated approach means that the same case might also be used to manage other notifications (like OSFI reporting or law enforcement contact) – while those are outside FINTRAC's scope, having everything in one case file is operationally convenient. **Built-in Audit Logs** record each step, from the time the name hit was generated to the time the report was filed, demonstrating timely compliance. On an ongoing basis, the **KYC 360° Dashboard** for any client will show if they are a sanctioned/PEP entity, providing front-line staff an immediate warning. Moreover, KROTON's watchlists are updated in real-time; the system can ingest new names (e.g. new persons added to a sanctions list overnight) and instantly rescreen, catching any hits that were previously customers. **In summary, KROTON keeps the institution in lockstep with sanctions obligations**: it conducts continuous screening (so listed persons are identified), manages the case investigation (so property is promptly frozen and isolated), and streamlines the reporting of terrorist property to FINTRAC. This end-to-end automation and documentation significantly reduce the risk of missing a sanctions hit or delaying a required report.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Sanctions & Terrorist Property Reporting (TPR/LPEPR)	• PCMLTFA s.7.1 (Report possession of terrorist-listed property) • Criminal Code s.83.1 / UN Act / SEMA (Listed person definitions via s.7.1)• OSFI/UN Sanctions Lists (screening obligation per guidance)	Sanctions Miner; Case Manager	Performs daily automated screening of clients and transactions against up-to-date sanctions and terrorist watch-lists (UN, OSFI, etc.). Flags any matches as alerts; Case Manager then facilitates immediate freezing of assets and creation of a Terrorist Property Report. The system auto-fills the report with client and account details and logs submission to FINTRAC. Sanctions Miner's continuous list

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
			synchronization ensures any newly listed person is caught and reported swiftly, keeping the institution fully compliant with sanctions and terrorist property reporting duties.

Compliance Program & Biennial Effectiveness Review

Regulatory Requirements: Finally, the PCMLTFA requires that every reporting entity establish and maintain an internal AML/ATF **Compliance Program** (PCMLTFA s.9.6(1)) . This program must include several key components as prescribed in the Regulations : (a) the appointment of a **Compliance Officer** who is responsible for the program; (b) the development of written **policies and procedures** to ensure compliance (approved by senior management and kept up-to-date); (c) a documented **Risk Assessment** of the entity's exposure to money laundering/terrorist financing risks (as discussed in the RBA section); (d) an ongoing **AML training program** for employees, agents and others acting on the entity's behalf ; and (e) an **effectiveness review** or audit of the compliance program conducted at least every two years, with the results reported to a senior officer/board . The biennial review can be done by internal or external auditors and must evaluate how well the compliance program is functioning – essentially testing the effectiveness of procedures, risk assessment, training, and reporting. Any deficiencies identified should be documented and addressed. Moreover, if significant changes (like new technologies or products) are introduced, the regulations require that the risk assessment be updated beforehand . FINTRAC examiners will typically ask to see evidence of all these program elements: the latest risk assessment report, training records, the compliance policies manual, the last two-year effectiveness review report, and proof of board approval and follow-up on that review. The overall expectation is that compliance is not a one-time effort but an ongoing, managed process with oversight and continuous improvement.

KROTON Platform Support: While KROTON is primarily a technology platform, it greatly aids in implementing and evidencing the compliance program. **Appointment of Compliance Officer:** KROTON usage can be aligned under the leadership of the designated compliance officer – the system's administrative settings can be managed by that person (or their delegates), ensuring top-level oversight of how the system is configured to meet policies. **Policies & Procedures:** Many of the institution's AML policies are effectively embedded in KROTON's rule configurations and workflows. For instance, if the written procedure says "screen all new clients for PEP and sanctions," KROTON's automated screening *is* that procedure in action. The platform can produce documentation of its configuration (scenarios, thresholds, etc.) which mirrors the institution's policies. **Training:** KROTON includes user guides and on-screen guidance which, combined with vendor support, forms part of staff training. Additionally, because KROTON automates complex tasks (like STR filing), it reduces the likelihood of staff error and the need for extensive manual training on how to file reports – the system guides them. Still, the institution should train staff on how to use KROTON, and KROTON's audit logs can show whether staff are appropriately using the system (e.g. are alerts being reviewed in a timely manner, etc.), which is an indirect measure of training effectiveness. **Biennial Review/Audit:** When it's time for an independent audit of the AML program, KROTON's comprehensive data retention is extremely useful. Auditors can be given read-only access or provided with exportable logs from KROTON: for example, a report of all alerts and their dispositions, all STRs filed, user activity logs, etc. This allows an auditor to objectively assess whether the transaction monitoring and reporting were done according to policy. KROTON's **Built-in Audit Logs** record every action (who reviewed what alert when, who approved which case, changes in risk scoring, etc.), which provides the evidence trail an auditor will sample . The system can also generate statistics and trend reports (number of STRs over time, training completion status if tracked, etc.) to inform the effectiveness review. Furthermore, if the program review finds a need to tighten a control (say, introduce a new scenario or adjust a threshold), KROTON can swiftly implement that change, and document it, thereby closing the loop between audit findings and program updates.

In summary, **KROTON acts as the technological backbone of the AML Compliance Program** – by embedding risk-based controls, facilitating oversight, and maintaining detailed documentation, it allows a compliance officer to run a robust program and readily demonstrate its effectiveness. The platform's contributions span every component of the program, ensuring that the institution not only complies in practice but can *prove* its compliance to FINTRAC and auditors with data and reports drawn from KROTON.

Compliance Area	Relevant Law/Guideline	H3M / KROTON Module(s)	How the Platform Supports Compliance
Compliance Program & Biennial Review	• PCMLTFA s.9.6(1) (Establish compliance program) • PCMLTFR 156(1) (Program components: Compliance Officer, Policies, Training, Risk Assessment, Effectiveness Review) • PCMLTFR 156(3) (Independent two-year effectiveness review requirement)	Case Manager; Scenario Manager; KYC 360° Dashboards; Built-in Audit Logs	Centralizes and enforces AML policies (via configured rules, workflows, and user permissions under the Compliance Officer's oversight). Serves as a training and execution platform – guiding staff through compliance workflows (reducing manual errors). Captures all compliance actions in audit logs and reports, which are utilized for the biennial effectiveness review. Scenario Manager and Case Manager statistics help measure program effectiveness (e.g. alert volumes, response times, STRs filed), and any needed adjustments to the program (new rules or process changes) can be swiftly implemented and documented within the platform. KROTON's comprehensive record-keeping provides the evidence required to demonstrate to auditors and FINTRAC that all program elements are active and effective.

Conclusion: By closely aligning its modules and functionality with FINTRAC's regulatory requirements, **KROTON** provides a powerful solution for compliance. Each major obligation under the PCMLTFA – from KYC and recordkeeping to transaction monitoring, reporting, and program governance – is actively supported and evidenced through the platform. This integrated approach not only helps ensure that no requirement is overlooked, but also creates efficiencies (automation and centralization) that allow compliance teams to focus on analysis and decision-making rather than tedious paperwork. Using KROTON, a reporting entity can confidently maintain a strong compliance posture and quickly adapt to evolving regulations or risk landscapes, all while demonstrably meeting the expectations of FINTRAC and other regulators. The mapping in this report illustrates that **KROTON's capabilities are well-matched to FINTRAC's AML/ATF compliance domains**, reinforcing that a technology-enabled compliance program can achieve both effectiveness and efficiency in safeguarding against financial crimes.

H3M Analytics Inc.

Finance Montréal, 4 Place Ville Marie Suite 300

Montréal, QC, Canada H3B 2E7