

WHITE PAPER



Re-engineering the Risk-Based Approach

Agentic AI as the engine of continuous risk assessment & control calibration

By Elizabeth Callan

For more than two decades, financial institutions have been instructed to adopt a “risk-based approach” (RBA) to anti-money laundering (AML) and financial crime compliance. Yet in practice, most programs remain largely static, rules-driven, and backward-looking. Risk assessments are typically conducted annually, threat information is consumed manually, and controls are slow to adjust to an increasingly dynamic financial crime landscape.

At the same time, financial institutions face an explosion of financial crime threat information - regulatory guidance, enforcement actions, typologies, public-private partnership intelligence, law enforcement advisories, sanctions updates, and open-source reporting. The challenge is no longer access to information, but the ability to continuously monitor, interpret, and translate that information into actionable risk insights.

Enter agentic AI. Combined with large language models (LLMs), agentic AI enables a shift from static risk scoring to continuous, intelligence-driven risk orchestration. This is not automation of AML tasks. It is a redesign of the operating model. Autonomously monitoring, synthesizing, and reasoning over vast volumes of financial crime threat data, agentic AI systems enable continuous risk intelligence - bridging the gap between threat awareness and operational decision-making. In doing so, they provide a practical pathway toward a truly risk-based AML framework.

The limitations of today’s “risk-based” AML programs

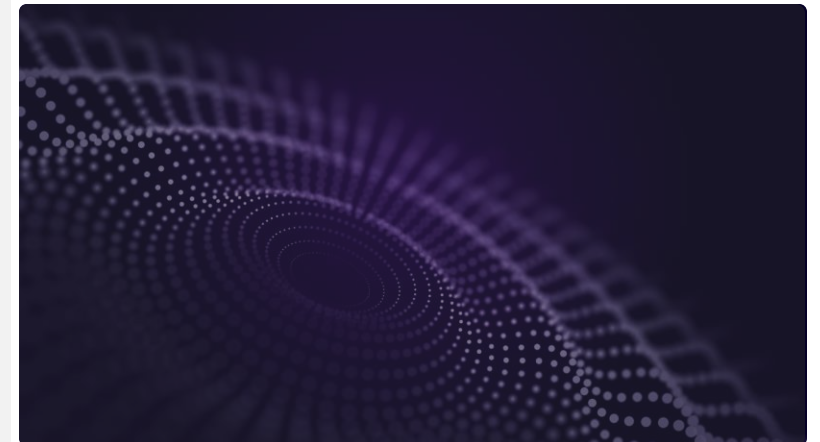
Most AML programs are risk-based in name, but not in execution. Several structural limitations persist:

- **Periodic risk assessments:** Enterprise-wide AML risk assessments are typically conducted annually or biannually, resulting in a static snapshot of risk that quickly becomes outdated.
- **Manual threat monitoring:** Compliance teams rely on human review of advisories, typologies, enforcement actions, and regulatory publications—an approach that does not scale.
- **Delayed control updates:** Changes to scenarios, thresholds, customer risk models, and due diligence standards often lag emerging threats by months or years.
- **Information silos:** Threat intelligence, transaction monitoring, sanctions, fraud, and investigations operate in parallel, with limited cross-pollination of insights.

The result is a compliance posture that is reactive rather than adaptive—focused on demonstrating procedural adherence rather than aligning controls with real-world financial crime risk. But this isn’t feasible for much longer.

“ Furthermore, as criminal networks continue to evolve at a rapid pace, as do national security priorities, FIs must embrace an innovation governance framework that is nimble and allows for prompt responses to evolving threats.

- *Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity, Part II: Transitioning to Innovation, August 2025*



The global push for a smarter risk-based approach

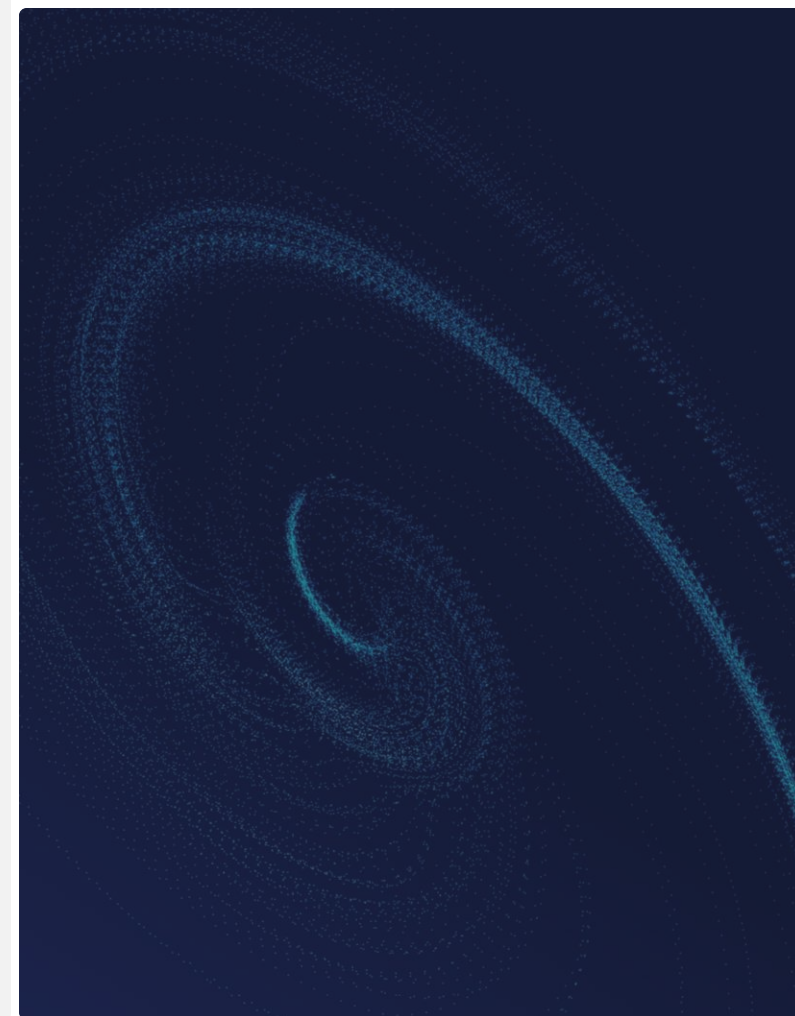
Global financial crime regulators and industry groups have consistently reinforced the RBA as the foundation of effective AML and sanctions compliance. The Financial Action Task Force (FATF), through Recommendation 1 and its ongoing guidance, continues to stress that both countries and financial institutions must apply resources and controls proportionally to actual risks rather than relying on a rigid, one-size-fits-all model. The group recently hosted a Learning and Development Forum on the RBA with more than 100 professionals across financial supervisors, financial intelligence units, law enforcement agencies, policy makers, and the Wolfsberg Group. In recent years, the FATF has placed greater emphasis on outcomes over process, urging a shift from purely procedural compliance to dynamic, intelligence-led, and measurable risk mitigation. It has also called on supervisors themselves to adopt risk-based supervision, focusing scrutiny on higher-risk entities and activities while encouraging innovation and proportionality. The Wolfsberg Group, representing many of the world's largest banks, reinforced these expectations in its July 2025 Statement, warning that many programs remain "risk-based in name only" and

calling for stronger public-private collaboration, smarter resource allocation, and a genuine transition to intelligence-driven, outcome-focused compliance.

At the national level, several major regulators have echoed and strengthened this message. In the United States, FinCEN and the federal banking agencies (OCC, FDIC, Federal Reserve) have increasingly highlighted the need for continuous risk assessment and adaptive controls, particularly in light of evolving threats such as sanctions evasion and fraud-linked money laundering. In 2024 and 2025, the United States took significant steps to modernize its AML framework. In June 2024, FinCEN issued a major Notice of Proposed Rulemaking (NPRM) aimed at strengthening and modernizing AML/CFT programs for financial institutions. The proposed rule emphasizes the RBA as the foundation of effective compliance. It would require banks and other covered institutions to conduct and maintain a risk-based AML program, including a regular, documented risk assessment that identifies, assesses, and mitigates money laundering, terrorist financing, and sanctions evasion risks specific to their business.

In Canada, FINTRAC has modernized its supervisory framework (August 2025) to prioritize a more sophisticated RBA, explicitly requiring reporting entities to integrate the 2025 National Risk Assessment into their own RBAs and demonstrate effective, evidence-based risk mitigation. In the United Kingdom, the FCA has

pushed firms to move beyond static risk assessments toward real-time risk understanding and better use of threat intelligence.



Enter agentic AI

A new compliance capability

Agentic AI refers to AI systems that can operate autonomously toward defined objectives by planning, executing tasks, and adjusting behavior based on feedback. Unlike traditional automation or point-in-time analytics, agentic AI systems can continuously observe their environment and act without constant human prompting.

When combined with LLMs, agentic AI becomes particularly powerful for RBA use cases. It can:

1. **Read and interpret unstructured text** (e.g., advisories, typologies, enforcement actions)
2. **Understand context**, intent, and risk relevance
3. **Synthesize insights** across disparate sources
4. **Reason about implications** for specific products, customers, geographies, and controls
5. **Generate structured outputs** aligned to AML frameworks

This capability directly addresses and automates one of AML's most persistent challenges: translating fragmented threat information into actionable, risk-aligned compliance decisions and control calibration.

Automating financial crime threat monitoring & translation

At the core of a risk-based AML program is an accurate understanding of current financial crime threats. Agentic AI systems can be designed to continuously monitor a wide range of internal and external sources, including:

- **Regulatory** and supervisory publications
- **Law enforcement** and FIU advisories
- **FATF** and regional body typologies
- **Enforcement actions** and consent orders
- **Sanctions** and export control updates
- **Open-source media** and litigation data
- **Public-private partnership intelligence** (where permitted)

Rather than simply ingesting this information, agentic AI can classify threats by typology, geography, product exposure, customer segment, and predicate offense. LLMs enable semantic understanding—distinguishing, for example, whether a new advisory signals an incremental refinement of an existing risk or the emergence of a materially new threat vector. This automation shifts threat monitoring from a manual, episodic activity to a continuous intelligence function.

Continuous threat intelligence & risk assessment

The true value of agentic AI lies not in information aggregation, but in **risk translation**. An agentic AI system can map emerging threats to an institution's specific risk profile by assessing relevance across dimensions such as:

- **Customer types** (e.g., MSBs, crypto firms, trade finance clients)
- **Products and services**
- **Delivery channels**
- **Geographic exposure**
- **Transaction volumes and behaviors**

This enables dynamic updates to risk assessments, transforming them from static documents into living risk models. Instead of asking, "What was our risk last year?", compliance teams can ask, "How has our risk changed this quarter—and why?" In this model, the risk assessment becomes a continuously refreshed output, supported by traceable threat intelligence and explainable reasoning.

Enabling adaptive controls and targeted resources

A truly risk-based approach requires that controls evolve in response to risk. Agentic AI can act as a connective layer between threat intelligence and control optimization by:

- **Flagging scenarios** that may require tuning based on new typologies
- **Identifying customer segments** that warrant enhanced due diligence
- **Highlighting geographies** where sanctions or corruption risks are escalating
- **Informing alert prioritization** and investigator focus
- **Supporting targeted training** and policy updates
- **Automating requisite changes** to policies and procedures

This approach supports regulatory expectations around proportionality—allocating resources where risk is highest, rather than spreading controls evenly across low- and high-risk areas alike—thereby also creating cost efficiencies for the business.

Figure 1.

Framework: The continuous risk assessment-control calibration cycle



Governance, explainability, and regulatory alignment

For agentic AI to be viable in AML, strong governance is essential. Systems must be transparent, auditable, and aligned with regulatory expectations. Key design principles include:

- **Human-in-the-loop oversight** for material risk decisions
- **Explainable outputs**, including source attribution and reasoning
- **Clear accountability** for AI-assisted judgments
- **Model validation and performance monitoring**
- **Segregation of duties** between intelligence generation and control execution

When implemented thoughtfully, agentic AI can enhance - not undermine - regulatory confidence by improving consistency, documentation, and traceability.

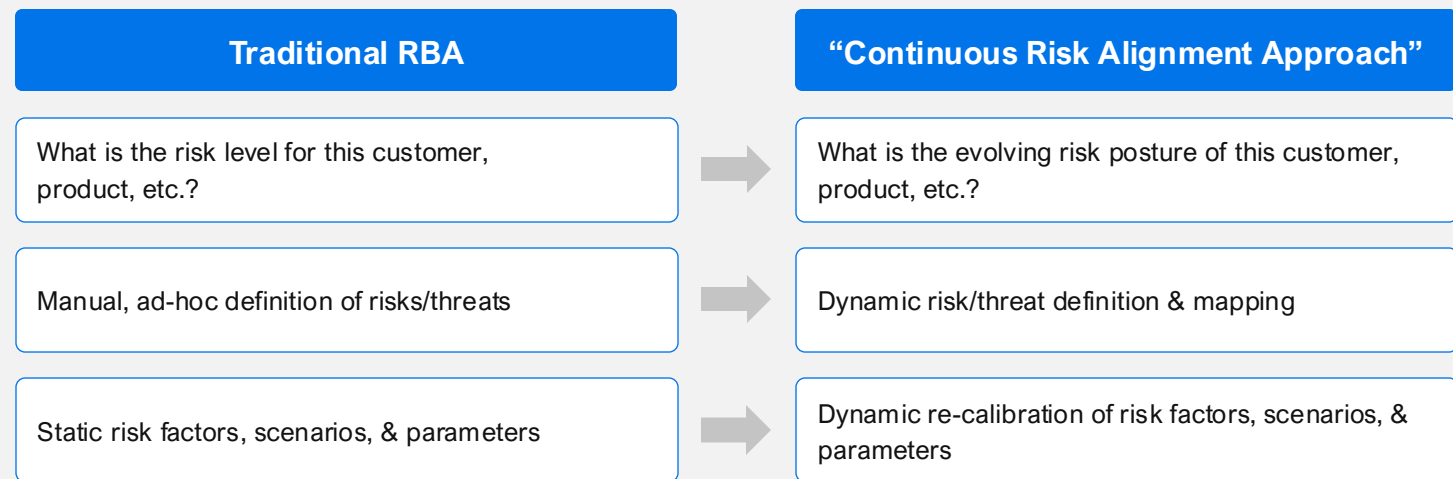
The strategic imperative

From periodic RBA to continuous risk alignment

A periodic, point-in-time risk-based approach is becoming increasingly difficult to sustain in today's financial crime environment. Threats evolve continuously—across geographies, products, and typologies—while traditional AML programs rely on annual assessments, manual intelligence gathering, and delayed control updates. This creates an inherent lag between emerging risks and institutional response. As a result, many programs are risk-based in design but not in execution, limiting their ability to effectively detect and mitigate real-world financial crime exposure and negatively impacting their bottom line.

Figure 2.

The strategic shift from the traditional risk-based approach to a “continuous risk alignment approach”



Agentic AI introduces a fundamentally different operating model by enabling continuous risk awareness and real-time translation of threat intelligence into actionable insights. By monitoring and synthesizing evolving financial crime signals, institutions can dynamically align controls with current risks, rather than historical assumptions. This not only improves detection effectiveness but also allows for more targeted allocation of resources—focusing effort where risk is highest. At the same time, enhanced transparency, traceability, and explainability strengthen regulatory defensibility, addressing growing supervisory expectations around effectiveness and accountability.

Looking ahead, the definition of a “risk-based” AML program is shifting. Regulators and stakeholders will place less emphasis on whether a framework exists, and more on whether it is demonstrably working in practice. The future state is one of continuous risk alignment—where institutions can show, in near real time, how their controls reflect the risks that matter most. In this model, compliance is no longer a periodic exercise, but an ongoing capability grounded in intelligence, adaptability, and measurable outcomes.

Conclusion

The financial crime threat landscape is dynamic, global, and increasingly complex. Static, manual compliance models are no longer sufficient to truly deliver a risk-based approach, meet regulatory expectations, or protect institutions effectively. Agentic AI and large language models offer a transformative opportunity: to move AML programs from periodic assessments and reactive controls to continuous risk intelligence and adaptive responses.

By automating the monitoring and interpretation of financial crime threats—and translating those insights into institution-specific risk—agentic AI makes the long-promised risk-based approach operationally achievable. In the next evolution of AML, the question will no longer be whether a program claims to be risk-based, but whether it can prove—continuously—that its controls reflect the risks that matter most.

*For a practical walkthrough of how agentic AI is implemented across the financial crime compliance lifecycle - including the agent ecosystem, architecture, and real-world workflow scenarios – see another release from SymphonyAI - **Agentic AI for Financial Crime Risk Management**.*

About the Author



Elizabeth Callan is a recognized leader and innovator in the fight against money laundering and financial crime with over 25 years of experience across intelligence, law enforcement, and the private sector.

At SymphonyAI, she is at the forefront of redefining the future of financial crime compliance and risk management. She drives strategy and innovation, developing groundbreaking AI-led, intelligence-driven solutions that are transforming how global institutions detect, disrupt, and prevent money laundering, sanctions evasion, and other sophisticated financial crimes. Her work is helping shift the industry approach from reactive, technical compliance to proactive, risk-aligned, and highly effective risk management.

Prior to SymphonyAI, Elizabeth served in the U.S. intelligence and law enforcement communities. As a Senior Intelligence Analyst at the U.S. Department of the Treasury, she shaped high-impact U.S. policy and enforcement actions — including Section 311 designations — while directly advising senior officials at OFAC and FinCEN on critical threats and national security strategies. She also served as Intelligence Liaison and Senior Advisor to the DEA's Special Operations Division, where she led complex, large-scale money laundering investigations, enhanced intelligence collection efforts, trained law enforcement agents and analysts, and forged strong international partnerships.

In the private sector, Elizabeth has held leadership roles in financial institutions and consulting firms, where she built and managed investigations teams, designed robust AML and sanctions programs, and developed risk management strategies for complex products and services.

A recognized subject matter expert, Elizabeth teaches AML and sanctions courses at the university level. She holds a master's degree in economics and the prestigious ACAMS Advanced Certification in Financial Crimes Investigations (CAMS-FCI).

About SymphonyAI

SymphonyAI, is building the leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, finance, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have 2000 leading enterprises as clients globally. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is an SAI Group company, backed by a \$1 billion commitment from Dr. Romesh Wadhvani, a successful entrepreneur and philanthropist.

SymphonyAI Financial Services provide AI-focused SaaS solutions developed from the ground up for compliance and financial crime risk management. An end-to-end offering compiled from more than 25 years of knowledge in tackling money laundering and fraud, our award-winning product ecosystem comprises an innovative and modern approach to financial crime investigation using world-leading agentic, predictive, and gen AI. From KYC/CDD and transaction monitoring through to payments fraud, entity resolution, and sanctions, PEP, and adverse media screening, SymphonyAI is a trusted name in finance technology with more than 200 financial institutions enjoying the power, efficiency, effectiveness and productivity that our solutions provide.

[Get in touch with us](#) to explore how agentic AI can enhance your risk-based approach and power effectiveness throughout your financial crimes risk management program.

Email us directly at connect.fs@symphonyai.com
Visit www.symphonyai.com

