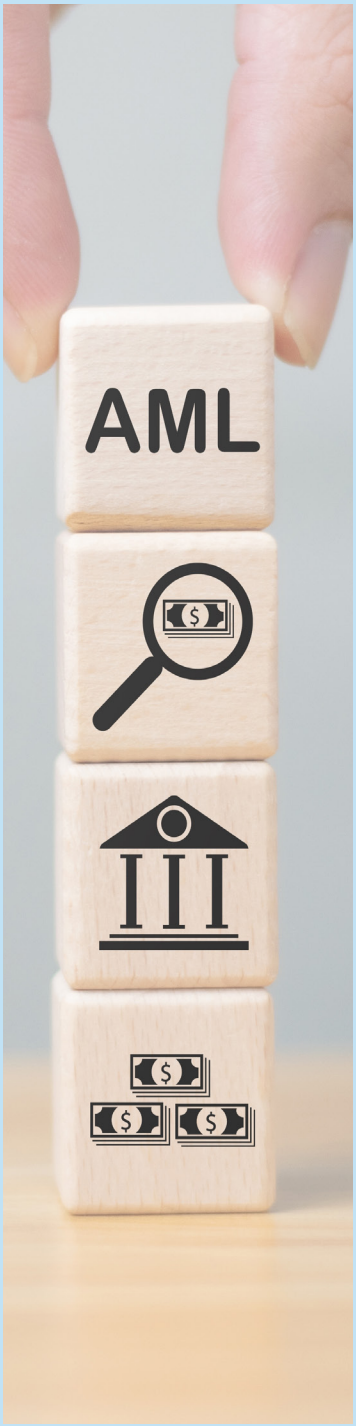
VIEW POINT



UNDERSTANDING THE RISK-BASED APPROACH IN AML FOR BETTER COMPLIANCE

Abstract

Unlike prescriptive compliance models of the past, the Risk-Based Approach (RBA) represents a fundamental shift in how financial crime compliance programs are designed and operated. Instead of treating all customers, products, and geographies equally, RBA focuses resources where risks are greatest. In doing so, it balances efficiency with regulatory rigour, making compliance smarter rather than heavier.

This article unpacks why RBA matters now, how organisations can conduct a strong AML risk assessment, the central role of Customer Due Diligence (CDD), and how governance, culture, and technology come together to sustain effective programs.

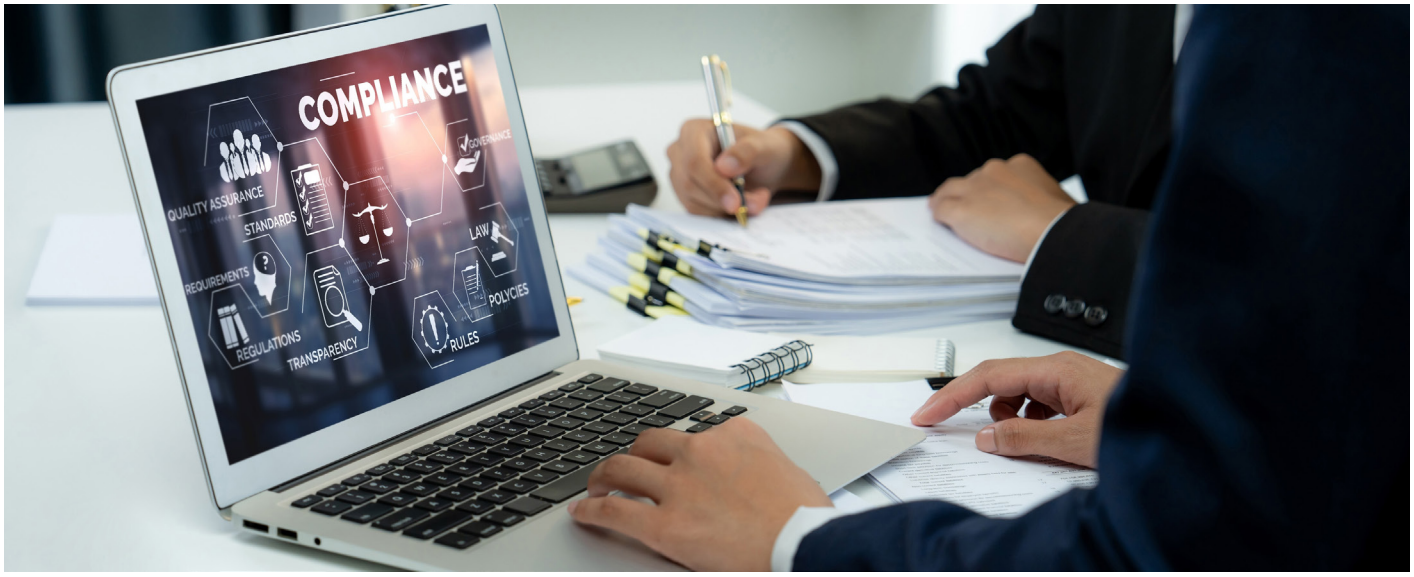
Infosys®
Navigate your next

Money laundering and terrorist financing remain serious global threats. The United Nations estimates that between 2% and 5% of global GDP annually is laundered through financial systems. Such illicit flows destabilise economies, undermine governance, and fuel organised crime and terrorism. Against this backdrop, regulators worldwide are making it clear: firms must adopt a risk-based approach in AML (Anti-Money Laundering) to remain both compliant and resilient.

This article explores the risk-based approach in AML as the global standard for combating financial crime. It also examines how governance, culture, and technology, especially AI, enable scalable, resilient compliance programs that balance efficiency with regulatory expectations.

Why does the risk-based approach matter now

The Financial Action Task Force (FATF) has long emphasised that the RBA sits at the heart of effective AML frameworks. By tailoring controls to actual risk levels, institutions not only satisfy regulators but also create operationally sustainable compliance programs. Given the urgency of evolving threats and regulatory demands, three major trends make the risk-based approach especially urgent today:



Rising enforcement actions

In 2023 alone, regulators issued more than $6.6 billion in fines globally, with the majority tied to weaknesses in Know Your Customer (KYC) and CDD processes. The takeaway? "One-size-fits-all" compliance programs can no longer stand up to scrutiny.

Evolving threats

The 2024 US National Money Laundering Risk Assessment spotlights risks from virtual assets, professional intermediaries, and trade-based money laundering, areas that demand nuanced, risk-sensitive responses.

Resource constraints

Compliance budgets continue to rise, but they are not limitless. Institutions must deploy staff, technology, and capital where they can achieve the most impact.

These forces converge on a single truth: adopting RBA is not simply about checking a regulatory box. It is about ensuring that compliance frameworks remain resilient in an environment where both risks and expectations are constantly shifting.

With that urgency established, the natural next question is: how can institutions bring this principle to life? The answer lies in a robust AML risk assessment.

AML risk assessment: the foundation of a strong risk-based approach

An AML risk assessment forms the backbone of any risk-based compliance program. It is the structured process through which organisations identify, measure, and prioritise money laundering and terrorist financing risks. Done well, it provides a map for where resources should be directed.

The process typically unfolds in three stages:

Identify risk factors

Products and services: Trade finance, correspondent banking, prepaid cards, savings accounts.
Customer types: Retail individuals, high-net-worth clients, corporates, trusts, or non-profits.
Geographies: High-risk jurisdictions, sanctioned countries, or underregulated markets.
Delivery channels: Digital-only platforms, in-person onboarding, or agent networks.

Assess likelihood and impact

Each risk factor is evaluated in terms of how likely it is to be misused and what the potential damage would be if it is. For instance, a multinational corporate client with complex ownership spanning multiple high-risk jurisdictions will inevitably carry more risk than a domestic retail customer with a simple profile.

Prioritise and apply controls

Risks are rated, low, medium, or high and linked directly to controls. High-risk profiles may trigger Enhanced Due Diligence (EDD), while low-risk customers may qualify for Simplified Due Diligence (SDD).

Most importantly, the risk assessment cannot be static. It should evolve whenever a new product is launched, a new market is entered, or when regulators issue fresh guidance. In this way, the risk assessment becomes a living compass that guides all compliance activity.
From this foundation flows the operational centrepiece of RBA: Customer Due Diligence.

Customer due diligence: turning risk insights into action

If AML risk assessments provide the strategy, Customer Due Diligence (CDD) delivers the tactics. CDD is how institutions put their understanding of risk into day-to-day practice, shaping how customers are onboarded, monitored, and managed.

Key elements include:

Risk-based onboarding: Customers are classified by risk at the outset, shaping how much scrutiny is applied

Standard CDD: Basic identification and verification suitable for most customers

Ongoing monitoring: Activity is tracked against expected behaviour, with alerts triggered for anomalies

Simplified Due Diligence (SDD): For low-risk profiles, simplified processes reduce cost and friction while maintaining compliance

Enhanced Due Diligence (EDD): Applied to higher-risk categories such as Politically Exposed Persons (PEPs) or entities with opaque structures, and this often includes source-of-wealth checks, adverse media screening, and senior management approval

Crucially, regulators now demand evidence that CDD practices align with the risk assessment. If an assessment flags exposure to shell companies, supervisors expect enhanced beneficial ownership checks to be built into onboarding and monitoring.

Yet, as customer bases grow and transactions multiply, managing CDD manually becomes untenable. This is where technology transforms RBA from principle into scalable practice.

Technology and AI: scaling the risk-based approach in AML

For global institutions with millions of clients, implementing RBA is highly impractical without technology. Manual processes alone cannot deliver the necessary precision or scalability.

Modern compliance programs increasingly rely on technology to:

Automate onboarding and verification

Digital KYC solutions, sanctions screening, and beneficial ownership checks reduce manual errors while speeding up processes.

Adjust monitoring thresholds

Transaction monitoring systems adapt alert thresholds to customer risk profiles, reducing false positives.

Leverage analytics and AI

Machine learning uncovers hidden networks and suspicious patterns that static rules might miss.

Centralise case management

Dashboards and workflow tools streamline investigations and document decision-making for audits.

According to industry reports, over 70% of financial institutions are boosting investment in AML technology, with AI and machine learning topping their priorities. The trajectory is clear: scalable, data-driven compliance is the future. Still, technology is only one piece of the puzzle. To succeed, it must be embedded within strong governance and a supportive culture.

Beyond technology: governance and culture in AML compliance

No technology can substitute strong governance and a healthy organisational culture. Regulators increasingly expect institutions to show not only that they have controls in place but that those controls reflect clearly defined responsibilities and values.

Governance essentials include:

- Clear accountability for risk assessments, policies, and oversight
- A board-level risk appetite statement that defines acceptable levels of risk
- Alignment between written policies and everyday procedures
- Metrics and regular testing to confirm effectiveness

Cultural elements matter just as much:

- Training staff to recognise red flags and apply judgment
- Empowering employees to escalate issues without fear
- Leadership signalling that compliance is a strategic priority, not a box-ticking chore

When governance, culture, and evidence align, institutions can demonstrate to supervisors that their RBA is both intentional and effective. But to sustain this, progress must be measured.

How to prove your AML risk-based approach works

For an RBA to remain credible, organisations must demonstrate outcomes, not just intentions. This requires tracking key performance indicators (KPIs) such as:

Coverage
Percentage of customers risk-scored at onboarding

Quality
Completion rates of EDD for high-risk clients

Efficiency
Ratio of false positives to true alerts; average case closure times

Outcomes
Reduction in regulatory findings; speed of remediation after audits

These metrics not only reassure regulators but also give boards confidence that resources are being used effectively. With measurement in place, decision-makers are better positioned to evolve their programs.

From theory to practice: AML risk-based approach tips for leaders

For leaders tasked with shaping AML strategy, five practical steps can strengthen implementation of the risk-based approach:

Start small, refine, then scale

Pilot in one geography or product, refine processes, and expand gradually.

Invest in data quality

Risk scoring and monitoring are only as reliable as the data they rely on.

Balance automation and human judgment

Let technology handle volume, while experts focus on complex cases.

Document everything

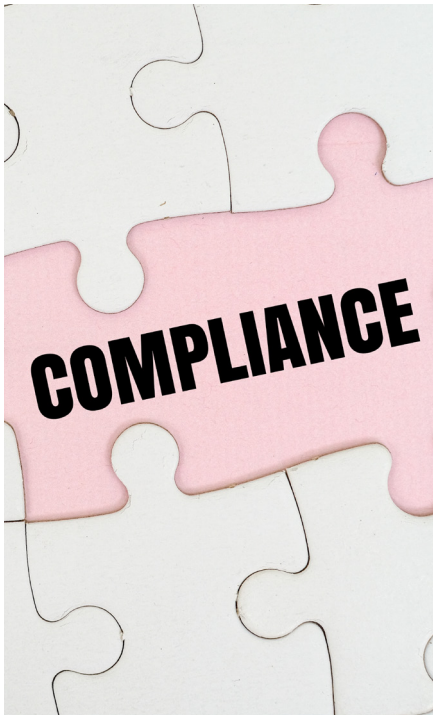
Regulators care as much about your reasoning as your results.

Embrace continuous improvement

Risks evolve quickly; so must your risk models and CDD practices.

By embedding these principles, firms can move from reactive compliance to proactive risk management.

The future of AML: what's next for the risk-based approach



The fight against financial crime is entering a new era. With global money laundering estimated at over $3.1 trillion, regulators worldwide are shifting to a risk-based approach in AML, requiring institutions to build smarter, more adaptive compliance frameworks. In the US, FinCEN's proposed rules emphasise risk assessments as the foundation of AML/CFT programs while encouraging innovation and technology adoption.

Generative AI is emerging as both a challenge and an opportunity. Criminals are exploiting it to scale fraudulent activities like shell company creation, but in the right hands, AI empowers investigators to analyse massive, unstructured data sets, accelerate case resolution, and reduce false positives.

Equally important is tackling predicate crimes such as drug trafficking, human trafficking, and terrorist financing. These upstream drivers of money laundering demand targeted detection strategies beyond conventional transaction monitoring.

Finally, the future depends on collaboration. Global reforms in regions like the EU and Canada, along with frameworks like Section 314(b) in the US, highlight the growing role of cross-institution and cross-border information sharing.

Future success lies in scaling AML compliance programs that combine risk-based assessments, AI-driven efficiency, and collaborative intelligence to outpace financial criminals.

Making the risk-based approach in AML your competitive advantage

The risk-based approach in AML is the global standard and the only way to keep pace with complex, fast-moving financial crime threats. At its heart lies a well-designed AML risk assessment, brought to life through proportionate Customer Due Diligence and enhanced by technology, governance, and culture.

When executed effectively, the RBA transforms compliance from a reactive burden into a proactive, strategic advantage. It allows firms to direct resources where they matter most, accelerate onboarding for legitimate customers, and reduce exposure to regulatory sanctions.

In an era where both regulators and criminals are raising their game, adopting a robust, technology-enabled risk-based approach is the surest path to resilient, future-ready compliance.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next