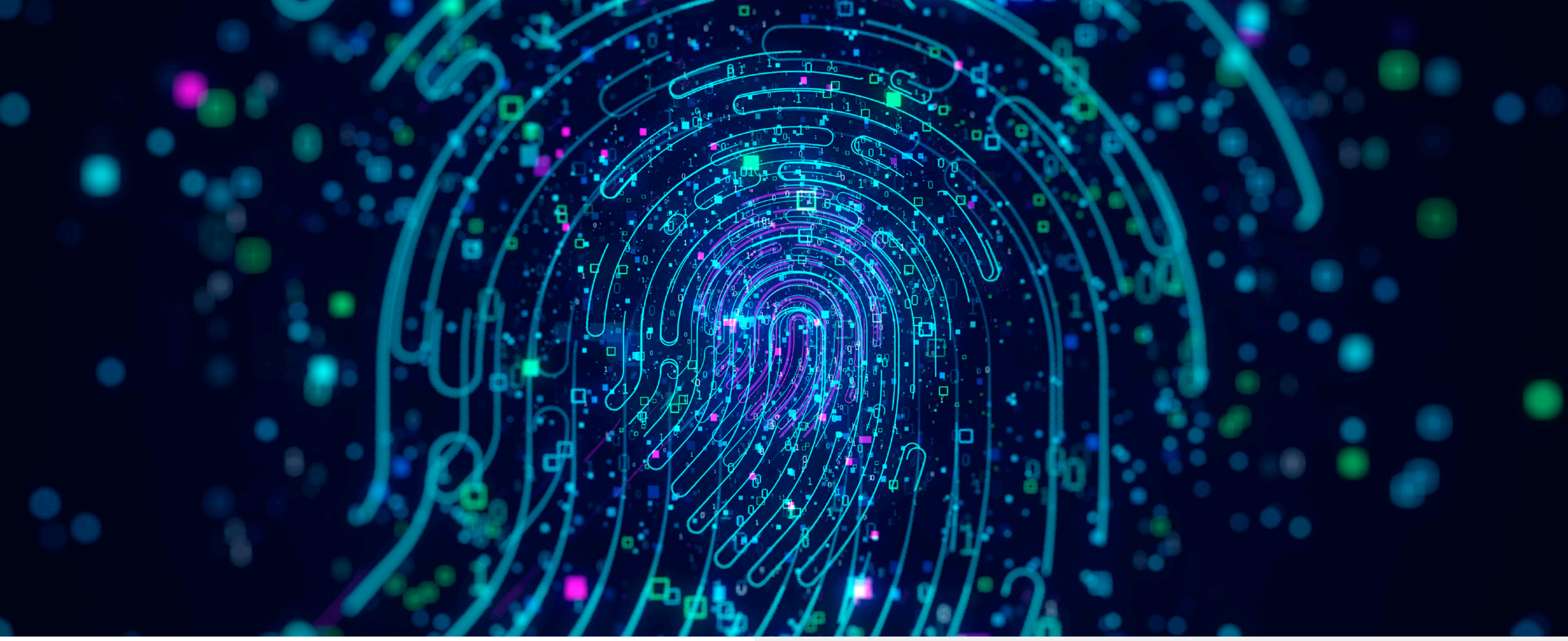
MOODY'S

KYC in context

A cross sector view of global regulatory frameworks



Know Your Customer (KYC) refers to the set of regulatory requirements and related processes used to identify and confirm the identity of customers, understand ownership and control structures, assess customer risk, and monitor customer relationships over time.

While KYC first emerged within banking, regulatory developments over the past decade have extended its scope across financial services and into a growing range of professional and non-financial sectors.

This paper outlines some of the key global regulatory frameworks that underpin KYC requirements and looks at how those frameworks apply across banking, asset management, insurance, and professional services. It brings together guidance and rules issued by the Financial Action Task Force (FATF), the European Union, US FinCEN, and the UK government, which collectively help influence how Customer Due Diligence (CDD) is defined and implemented worldwide.

FIVE GLOBAL REGULATORY FRAMEWORKS GOVERNING KYC PROCESSES

Below is a list of five key pieces of global regulatory guidance and legislation that directly underpin KYC processes. These are some of the foundational frameworks that inform KYC and CDD obligations globally across banks, asset management, insurance, professional services, and other regulated entities.

1. FATF Recommendations: Recommendation 10 (Customer Due Diligence)

Issuer: Financial Action Task Force (FATF)

WHY IT MATTERS:

- → This is essentially a global reference point for KYC and CDD.
- → Requires identification and verification of customers, beneficial owners, ongoing monitoring, and enhanced due diligence (EDD) for higher-risk customers.
- → Most national KYC frameworks are aligned with or informed by FATF Rec. 10.

2. EU Anti-Money Laundering Directive (AMLD): CDD/KYC Requirements

Issuer: European Union

WHY IT MATTERS:

→ Establishes unified CDD, EDD, and ongoing monitoring requirements for all EU-regulated entities.

→ Applies to financial institutions and designated non-financial businesses and professions (DNFBPs).

→ Forms a legal basis for EU identity verification and risk-based KYC.

3. U.S. Customer Due Diligence Final Rule (FinCEN CDD Rule) Requirements

Issuer: U.S. Department of the Treasury, FinCEN

WHY IT MATTERS:

→ Requires identification and verification of beneficial owners of legal entities.

→ Strengthens KYC expectations for banks, broker-dealers, mutual funds, futures commission merchants, etc.

→ Represents a key component of the U.S. framework for implementing risk-based CDD obligations.

4. U.S. Customer Identification Program (CIP) Requirements (BSA / USA PATRIOT Act §326)

Issuer: U.S. Treasury (via FinCEN), with CIP rules typically issued jointly with relevant federal functional regulators; FinCEN can issue rules directly where no such regulator exists.

WHY IT MATTERS:

→ Mandatory KYC requirement to identify and verify customers before account opening.

→ Applies to banks, credit unions, broker-dealers, and in 2028, investment advisers.

→ Defines minimum data collection (name, address, DOB, ID number), verification, and risk-based procedures.

5. UK, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17)

KYC/CDD Rules, with an amendment in 2019 to incorporate the EU's 5th Money Laundering Directive to strengthen and expand CDD. This expanded the scope of regulated entities (e.g., crypto asset exchange providers, custodian wallet providers, art market participants).

Issuer: UK Government: HM Treasury

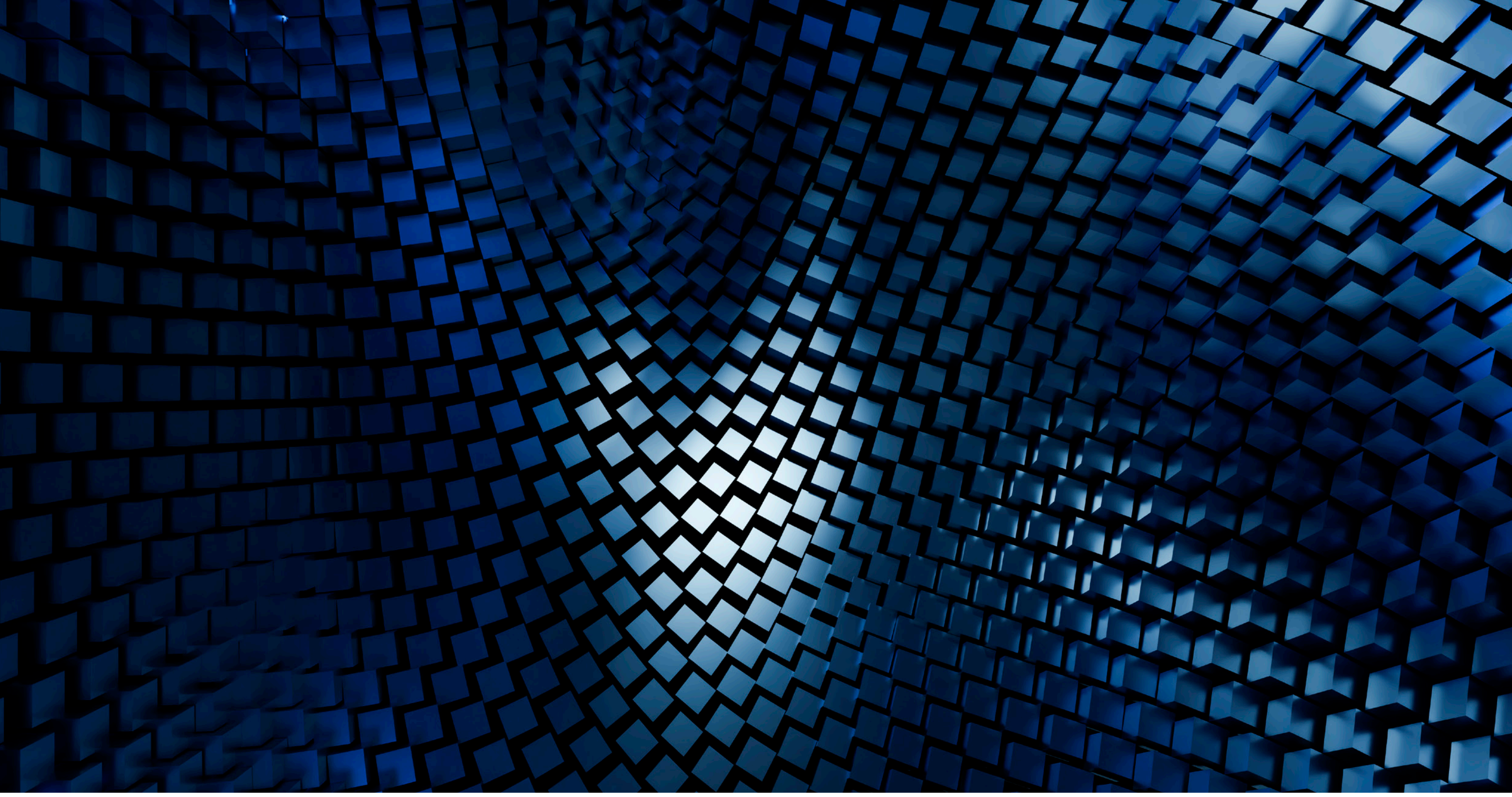
Supervision and monitoring: Compliance with MLR 2017 is overseen through a sector based AML supervisory framework in the UK, with ongoing monitoring requirements assessed by relevant regulators (including the FCA, HMRC, and other statutory bodies depending on firm type). This approach is intended to support a more consistent application of KYC and CDD obligations across financial and non financial sectors.

WHY IT MATTERS:

→ Implements CDD, EDD, ongoing monitoring, and beneficial ownership checks across the UK financial and professional services sectors.

→ Aligns UK KYC requirements with FATF standards while reflecting domestic risk priorities.

→ Covers verification obligations for both natural and legal persons.



Heat Map summary

✓ Green = “Strong, explicit regulatory applicability”

✓ Orange = “Partial or risk-based applicability”

ONBOARDING

Requirement	FATF	EU	US	UK
Identify Customer	✓ Green	✓ Green	✓ Green	✓ Green
Verify Identity	✓ Green	✓ Green	✓ Green	✓ Green
Beneficial Ownership	✓ Green	✓ Green	✓ Green	✓ Green
Risk Assessment	✓ Green	✓ Green	✓ Green	✓ Green
Enhanced Due Diligence	✓ Green	✓ Green	✓ Orange	✓ Green

ONGOING MONITORING

Requirement	FATF	EU	US	UK
Ongoing Monitoring	✓ Green	✓ Green	✓ Green	✓ Green
Customer Due Diligence	✓ Orange	✓ Green	✓ Orange	✓ Green
Transaction Monitoring	✓ Green	✓ Green	✓ Green	✓ Green

Table: Some similarities and differences in global KYC requirements

LEGEND:

→ ✓ **Similarity** i.e., requirements aligned across frameworks

→ Δ **Difference** i.e., requirements vary significantly

Requirement	FATF	EU AMLD	US (FinCEN CDD + CIP)	UK (MLR 2017)	Similarity / Difference
Identity Verification (Customer ID)	Requires identification & verification before relationship begins	Mandatory CDD at onboarding	CIP requires identity verification before account opening	Mandatory ID verification at onboarding	Strong alignment across all frameworks ✓
Beneficial Ownership (BO) Checks	Required under Recommendation 10	Required for all obliged entities (incl. accountants & tax advisers)	FinCEN's CDD Rule mandates BO identification for legal entities	BO checks required for all MLR-regulated entities	Strong alignment globally ✓
Risk-Based Approach (RBA)	Core FATF principle; risk-based CDD required	Required across EU obliged entities	Required across CDD + CIP processes	Required across MLR 2017	Universal requirement ✓
Enhanced Due Diligence (EDD)	Required for high-risk customers/events	Required, including for high-risk sectors and activities	Only required in certain risk-triggered cases (less prescriptive, for example applicable to Foreign Correspondent Banking & Private Banking for non-US person).	Requires EDD for high-risk customers, firms, geographies	US less prescriptive; others more explicit Δ
Ongoing Monitoring	Required for all relationships; review triggers update obligations	Mandatory ongoing monitoring	Required as part of BSA AML expectations	Required across all regulated sectors	Strong alignment globally ✓
Trigger for CDD Refresh	Required when risk changes or anomalies detected	Required as part of lifecycle monitoring	Required when new risk-relevant info emerges	Required for ongoing monitoring & EDD cases	Broadly similar, minor differences ✓
Legal Structure of Requirement	Non-binding standards applied globally via national law	Legally binding directives/ regulations across EU	Binding federal regulation (BSA + FinCEN rules)	Binding UK domestic legislation (MLR 2017)	FATF = standards; others = enforceable via national laws Δ

Why each sector is thinking about who they are doing business with

A decade ago, KYC was widely seen as a banking task: a checklist to complete before opening an account. Today, that view has changed.

From a mid-tier bank onboarding cross-border corporates to a global asset manager launching a new fund, to an insurer distributing products through independent brokers, to a law or accounting firm advising on complex transactions – KYC has become a lifecycle obligation that cuts across sectors and client relationships.

This isn't happening by accident. It's being driven by a convergence of global regulatory frameworks, and here are some examples:

→ The FATF Recommendations, which serve as a global reference point for customer due diligence (CDD), identity verification, beneficial ownership checks, and ongoing monitoring.

→ The EU's Anti-Money Laundering Directive (AMLD) and the new AML Regulation (AMLR), which set out CDD and monitoring duties for "obliged entities" – not only financial institutions but also auditors, external accountants, and certain legal professionals.

→ The US FinCEN Customer Identification Program (CIP) rules and CDD Final Rule that require banks and other covered institutions to identify and verify customers and beneficial owners before opening accounts.

→ The UK Money Laundering Regulations 2017 (MLR 2017), which extends CDD, beneficial ownership checks and ongoing monitoring across financial firms and supervised professional services.

1. FATF RECOMMENDATIONS (GLOBAL)

Sector	Applicable
Banking	✓
Asset management	✓
Insurance	✓
Professional services (e.g., law firms, accountancies, consultancies)	✓

2. EU AMLD (EU ANTI-MONEY LAUNDERING DIRECTIVE)

Sector	Applicable
Banking	✓
Asset management	✓
Insurance	✓
Professional services	✓

3. US FINCEN (CDD RULE + CIP)

Sector	Applicable
Banking	✓
Broker-dealers in asset management	✓
Insurance – covered insurers only	✓
Professional services	✗

4. UK MONEY LAUNDERING REGULATIONS 2017 (MLR 2017)

Sector	Applicable
Banking	✓
Asset management	✓
Insurance	✓
Professional services	✓

Let's look at how the story plays out, sector by sector.

Chapter 1: Banks who can't afford to just 'tick the box'

The story starts where KYC first took root: in banking.

Global and regional banks sit squarely in the sights of major KYC and AML frameworks. Under FATF Recommendation 10, banks are treated as financial institutions that are expected to identify and verify customers and beneficial owners, understand the nature and purpose of the relationship, and monitor accounts for potentially suspicious activity.

In the EU, banks are "obliged entities" under the AMLD, with a harmonized framework for CDD, enhanced due diligence (EDD), and ongoing monitoring.

In the US, CIP rules require banks and other covered financial institutions to collect and verify key identifiers before opening accounts, while the FinCEN CDD Rule obliges them to identify and verify beneficial owners of legal entity customers at account opening.

Recent developments in the U.S. further illustrate how KYC and AML expectations evolve. In April 2026, FinCEN issued a notice of proposed rulemaking (NPRM) to reform AML/CFT program requirements under the Bank Secrecy Act. The proposal signals a shift toward evaluating whether AML programs are operating in a risk-based and reasonably effective manner, with greater emphasis on how institutions assess and prioritize risk, rather than solely on procedural adherence.

It also introduces further distinctions between the design of a program and how it is implemented in practice, alongside expectations that firms allocate attention and resources aligned to higher-risk customers and activities. If finalized, the changes would align U.S. supervisory expectations more closely with other international principles that emphasize risk-based approaches and ongoing monitoring across the customer lifecycle.

More broadly, a recent US Financial Integrity Executive Order points toward continued strengthening of AML and KYC expectations, including greater emphasis on customer identification, beneficial ownership, and risk assessment frameworks.

Switching to the UK, banks are required to comply with MLR 2017, applying risk based CDD and ongoing monitoring across their customer base.

For a bank, these evolving principles and requirements mean KYC is not a static file captured at onboarding. It's one foundational element for risk-based relationship management. New products, new geographies, new counterparties, and changes in ownership are often reflected in dynamic customer risk profiles, supported by robust data on identity, beneficial ownership, sanctions exposure, adverse media, and more.

Chapter 2: Asset Managers who know investors are only half the story

Next, we move to the buy-side.

Asset managers have historically focused on investor suitability, distribution agreements, and fund documentation. But regulators are now expecting greater AML and KYC alignment with banks, especially for products that attract cross-border flows or complex holding structures.

Under FATF, asset management fits within the definition of "financial institutions" subject to CDD obligations.

The EU AMLD designates asset managers as obliged entities, introducing CDD, EDD and monitoring obligations over investors and certain intermediaries.

In the US, mutual funds are specifically named in the FinCEN CDD Rule.

And UK asset managers fall under MLR 2017 as financial institutions.

The result of this is that fund managers may increasingly need to look beyond basic name-screening at subscription toward:

→ Identifying who is behind the investment, including beneficial owners and controlling interests.

→ Assessing and categorizing investor risk using a risk-based approach, not just product questionnaires.

→ Monitoring changes in behavior or ownership that could indicate higher risk over time.

This can lead asset managers toward the same kind of KYC, and ongoing monitoring infrastructure banks have been building, but with nuances around distributors, platforms, and complex fund structures.

Chapter 3: Insurers and Brokers realizing policies can be used as payment rails

Insurance has often been viewed as lower risk than transactional banking. But for life and investment-linked products, regulators increasingly see a similar risk profile: money in, money moved, money out, sometimes across borders and over long timeframes.

Under FATF, life insurers are included within the scope of financial institutions subject to CDD rules.

In the EU, insurance undertakings offering life insurance or other investment-related services are obliged entities under AMLD, with applicable CDD and monitoring obligations.

And in the UK, those same insurers are subject to MLR 2017 requirements for CDD, beneficial ownership checks, and ongoing monitoring.

For insurers, the risk lens is different, focusing on:

- → The identity and risk profile of policyholders and beneficiaries
- → The behavior of distributors and intermediaries
- → Indicators like unusual premium patterns, policy transfers, or early surrenders

To manage that risk, insurers may consider KYC and AML capabilities that can support a more holistic view between the customer, the product, and behavior over time, not just at inception.

Chapter 4: Professional Services firms who became front-line AML gatekeepers

A striking change in the global KYC story is the rise of professional services firms, i.e., law firms, accounting practices, tax advisers, and trust and company service providers, as explicit AML-regulated entities.

The FATF recognizes these as Designated Non-Financial Businesses and Professions (DNFBPs) and recommends countries regulate them in a similar manner to financial institutions, with risk-based and proportionate CDD and monitoring obligations.

The EU AMLR goes further, explicitly designating auditors, external accountants, and tax advisers — and, in defined circumstances, legal professionals — as obliged entities who are required to apply CDD and submit suspicious activity reports where applicable.

In the UK, guidance by HM Revenue and Customs on "who needs to register for money laundering supervision" says that firms providing audit, accountancy, tax advice, and certain legal or trust and company services fall within the scope of MLR 2017.

In practice, that means professional services firms may be expected to:

- → Perform CDD before accepting engagements
- → Identify the beneficial owners behind corporate and trust structures
- → Screen for PEPs, sanctions, and adverse media
- → Monitor higher-risk clients and matters on an ongoing basis

And for their own clients (banks, asset managers, corporates), these firms themselves often become important third parties who may need to be risk-assessed and monitored.

Chapter 5: One regulatory story. Many risk use cases

Taken together, these developments tell a story that KYC is no longer just a banking task. It is a cross-sector, cross-lifecycle discipline that supports AML compliance and third-party risk management.

→ FATF provides a global reference point for CDD, beneficial ownership, and ongoing monitoring across financial institutions and DNFBPs.

→ The EU AML framework translates that baseline into detailed, harmonized requirements for banks, asset managers, insurers, auditors, accountants, and certain legal professionals.

→ US FinCEN rules make identity verification, and beneficial ownership checks core regulatory conditions for opening and maintaining financial relationships.

→ UK MLR 2017 extends similar duties across financial services and professional firms, backed by UK-specific supervisory controls.

For organizations operating across borders, or those serving customers who do, the implication is that a unified, data-driven view of who you are doing business with, what their risk profile is, and how that risk evolves over time can be important.

That's an area where advanced KYC, supplier risk, and AML solutions come in:

→ Helping bring together identity data, beneficial ownership, sanctions, PEPs, and adverse media

→ Applying a risk-based lens that is informed by FATF, EU, US, and UK expectations

→ Supporting ongoing monitoring rather than one-off checks

In other words: turning regulatory pressure into an opportunity to better understand counterparties and help demonstrate to regulators, customers, and investors that financial crime and third-party risk are a priority.

The scope and implications of KYC-related regulation

KYC requirements are shaped by a set of globally recognized regulatory frameworks that, while implemented through different legal regimes, generally reflect a consistent underlying approach. Across FATF, EU, US, and UK standards, regulators place emphasis on understanding customer identity, ownership, and control, assessing risk on a proportionate basis, and maintaining oversight as relationships evolve.

This paper illustrates that these expectations don't apply solely to banks. Asset managers, insurers, and professional services firms are increasingly within scope. Changes in regulation also mean an expansion of scope to crypto asset exchange providers and custodian wallet providers; and even sporting organizations or participants in the art market may also fall within EU, UK, and FATF scope. And broader policy initiatives focused on integrating financial technology and digital assets into regulated financial systems may, over time, extend the range of entities operating within frameworks where KYC and AML obligations apply. These developments reflect the role these sectors play in facilitating financial activity, managing value over time, or acting as intermediaries in complex structures.

In parallel, KYC obligations have expanded beyond initial onboarding to encompass ongoing monitoring, and the ability to explain or document how risk-based judgements are made and updated.

While the application of KYC varies by jurisdiction and sector, the direction of travel is broadly aligned. Regulators appear to be focused on consistency, transparency, and the use of reliable information to support CDD and AML oversight. For organizations operating across borders, this creates a shared regulatory reference point, alongside practical challenges in managing data, ownership complexity, and changing risk profiles.

Understanding the landscape of KYC-related regulation may be the first step.

Moody's solutions for KYC-related processes

As KYC requirements continue to apply across jurisdictions and sectors, organizations are increasingly expected to be able to articulate a clear, evidence-based understanding of who they are doing business with and how related risks may evolve over time. In this context, Moody's solutions support firms by providing data, analytical context, and workflow capabilities that can be informed by widely adopted regulatory frameworks.

Moody's solutions help bring together data relevant to KYC, AML, and CDD, including identity and entity data, ownership and control structures, sanctions and politically exposed persons (PEPs), and adverse media. These datasets can be used to support risk-based assessments informed by FATF principles and their implementation across EU, US, and UK regulatory regimes.

Beyond initial onboarding, Moody's capabilities can be used by organizations seeking to maintain regularly updated customer and counterparty profiles as relationships, ownership structures, and external risk indicators change. This reflects the regulatory emphasis on ongoing monitoring, or so-called "perpetual KYC," rather than point-in-time checks.

Moody's solutions can be applied across sectors, including banking, asset management, insurance, and professional services. In each case, they can support businesses working toward a more consistent approach to CDD, third-party assessment, and AML-related risk oversight, while being flexible to sector-specific considerations such as intermediaries, distribution models, or complex legal structures.

By providing a more unified view of identity, ownership, and external risk signals, Moody's data supports organizations in helping illustrate how KYC-related insights are sourced, assessed, and maintained. This can help organizations respond to supervisory queries, support internal governance, and navigate cross-border regulatory expectations.

Moody's solutions can play a supporting role in the KYC ecosystem, helping organizations to interpret and operationalize regulatory requirements through data, context, and analytical insight.

For more information, please get in touch with the team at any time.

Contact us

AMERICAS

+1.212.553.1658
clientservices@moodys.com

EUROPE

+44.20.7772.5454
clientservices.emea@moodys.com

ASIA (Excluding Japan)

+85.2.2916.1121
clientservices.asia@moodys.com

JAPAN

+81.3.5408.4100
clientservices.japan@moodys.com

BX_6639