MOODY'S

Who are you doing business with?

A MOODY'S STUDY INTO ENTITY VERIFICATION

moodys.com

KEITH BERRY

Executive summary

One of the key strategic goals of Moody's compliance and third-party risk management solutions is to help our customers answer the question – who am I doing business with? It's a deceptively simple question that can be very complicated to answer.

I'm excited to present the findings of our latest study on Entity Verification, as Entity Verification is crucial to understanding risk across your third-party business network, establishing trust, managing threats, and capitalizing on opportunities.

In today's ever-evolving business landscape, the importance of knowing who you are doing business with cannot be overstated. Economic and geopolitical uncertainties, stringent compliance rules, and the challenges of data management have heightened the need for robust Entity Verification practices.

Our research highlights the critical role Entity Verification plays in effective risk management and compliance. With global business interconnectivity, scrutiny from senior leaders on the importance of knowing your business partners, and a dynamic regulatory landscape, the requirements to "get this right" are pronounced.

For me, the study underscores the growing significance of Entity Verification data and harnessing that data to leverage it across an organization – beyond risk and compliance – to manage financial crime and prevent fraud of course, but to also drive operational efficiencies, and the imperative of customer experiences.

Despite the challenges posed to many by data quality limitations and the elusive goal of achieving a single customer view, leading companies with advanced data governance can create "golden records," and are then better positioned to achieve competitive advantage, manage compliance, and control risk.

Finally, I was excited to see the journey our audience has been on when it comes to the rising adoption of artificial intelligence (AI) in Entity Verification. This is a topic we're passionate about at Moody's, developing our own intelligent screening solutions using machine learning and launching our GenAI (generative artificial intelligence) research assistant. Again, the effectiveness of these new technologies hinges on data.

Circling back to where I started, helping our customers answer the question – who am I doing business with? How do you answer a simple question, well the simple answer is with data. The way that's accessed, screened for insights, managed, and controlled is a massive lever for success.

I hope you enjoy the report and I look forward to many more conversations on Entity Verification with you in the future.

Keith Berry

General Manager,
Moody's Compliance and Third-Party Risk Management Solutions

SECTION ONE

About the research

CONTEXT & OBJECTIVES

If you're a business operating in the global economy, how can you be sure who you're working with? It is a question that compliance teams have always had to answer, but one that is of growing importance as regulations across the world become more rigorous and complex. Is there an unscrupulous actor lurking in the shadows? Is a company you're dealing with exploiting forced labor? Entity Verification is crucial to understanding the legitimacy of a business and the risks across a company's third-party network. It helps establish trust, manage threats, and capitalize on opportunities.

Thinking about Entity Verification in a context of complex threats, sanctions continue to target a broad spectrum of actors, including states, organizations, and entities, as well as individuals. These individuals try hard to avoid the compliance net and clandestine networks are established to keep key information hidden. Sanctioned individuals can, for example, use a web of legal business structures, often in the form of shell companies, to obfuscate ownership.

Firms, and especially compliance teams within those firms, walk a precarious financial and reputational tightrope. If they get the decision wrong one-way, valuable business could be lost. If they get things wrong in another sense, senior leaders in the organization could face fines, damage in the market, or even prison.

Added to this, risks across the world are rising exponentially, becoming more widespread, interconnected, and difficult to pin down. From understanding each company across a supply chain to ESG (Environmental, Social, and Governance) risks or rapidly changing sanctions arising from geopolitical instability – companies must get deeper into the detail of knowing who they are working with to uncover the threats hiding across their business network.

We wanted to get deeper insight into the challenges and opportunities companies face in the field of Entity Verification, used to help identify and establish the legitimacy of a business. So, we conducted an indepth primary study to explore:

- To what extent Entity Verification as a topic is understood by organizations across financial and non-financial sectors.
- How important people perceive Entity Verification to be today and how that will change in the next two years.
- How companies rate the quality of their internal entity data, and the maturity of their data governance strategies.
- How close companies are to having a single customer view and establishing a 'golden record.'
- Key challenges and barriers faced by companies in Entity Verification.
- The extent of AI adoption, and the role Entity Verification is expected to play in supporting the rollout of AI.

METHOD

We partnered with market research specialists, Context+, who designed, conducted, and interpreted both quantitative and qualitative research on our behalf as an independent third-party.

We ran a comprehensive study which featured a detailed online survey gaining 310 responses from individuals across the world. We followed this up with 30 one-to-one in-depth interviews featuring risk and compliance professionals in financial and non-financial organizations to add richness and detail.

SAMPLE

Our study was global with respondents located in 50 countries across the Americas, Europe and Africa, Asia Pacific, and the Middle East. Our research spanned professionals working in the financial space, across banking, asset management, fintech and insurance, as well as non-financial organizations, including corporates, professional services, and government bodies, to provide the breadth of coverage that forms the basis of this paper.

PHASE ONE
Online survey

Sector	Americas	Europe & Africa	APAC & Middle East	Total
Financial Services (NET)	**56**	**88**	**49**	**193**
Banking	32	51	33	116
Asset & wealth management	7	11	3	21
Fintech	7	16	10	33
Insurance	10	10	3	23
Non-Financial Services (NET)	**47**	**51**	**19**	**117**
Corporates (Non-financial)	29	32	13	74
Professional services	14	15	4	33
Government & public sector	4	4	2	10
Total	**103**	**139**	**68**	**310**

PHASE TWO
One-to-one interviews

Sector	Americas	Europe & Africa	APAC & Middle East	Total
Financial Services	**3**	**8**	**2**	**13**
Non-Financial Services	**7**	**8**	**2**	**17**
Total	**10**	**16**	**4**	**30**

SECTION TWO

Adapting to uncertainty

THE MACRO PICTURE

Risk management and compliance have become more challenging and subsequently more sophisticated in the years following the 2008 financial crisis, the Panama papers, Russia's invasion of Ukraine and unprecedented rates of fraud as large swathes of the world's economy went digital. It's a response to the growing complexity, interconnectedness, and risks at the heart of the world's politics and economic systems.

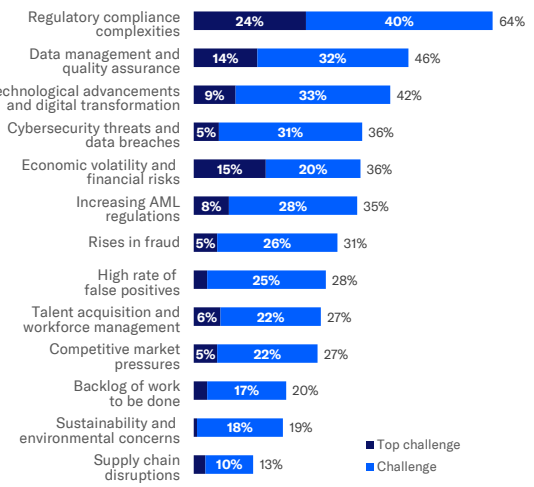
The spread of digital technology has created new ways to monitor risk, but also new ways to pose threats. Business is more global than ever, but subsequently, economic instability in one region can quickly spread to another. And as we have seen in recent years in Ukraine and the Middle East, geopolitical instability can reverberate around world.

This has led to more regulation, and a more complex risk and compliance landscape. And it has increased the chances of organizations coming into contact with sanctioned entities.

TRACKING THE TOP COMPLIANCE TEAM CONCERNS

Risk and compliance is a challenging environment to work in with many dynamic and growing problems to get to grips with. To set the context, we wanted to understand the key business challenges people in the field experience today.

TOP CHALLENGES AND CHALLENGES – TOTAL



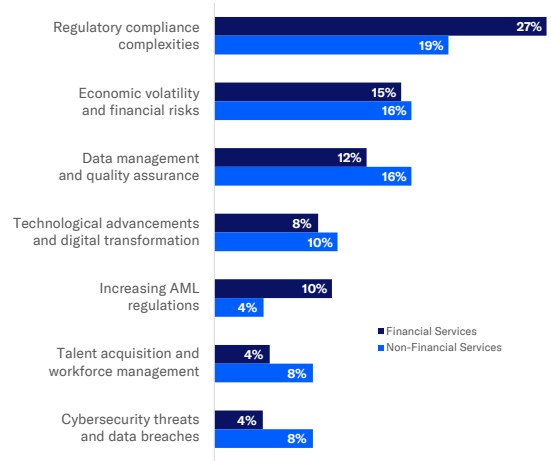
Regulatory compliance complexity was the most mentioned challenge, with 64% of people reporting it and 24% choosing it as their single most important issue. This was followed by data management and quality assurance issues, cited by 46% of people in total and 14% as their top issue.

Technological advancement and digital transformation at 42% was next. Cybersecurity and data breaches were mentioned by 36% of people, while economic volatility and financial risks were also cited by 36% of respondents, with 15% mentioning it as their top concern. This highlighted a key challenge that people faced which ran throughout our research.

> **"Overall, regulatory compliance complexity is our single biggest challenge. The complexity of regulations cascades down into a lot of our other issues."**
>
> Managing Director, Professional Services, UK

When we break down people's top concerns between financial and non-financial sectors, we also see some illuminating results. Financial services companies are more likely to cite regulations and Anti-Money Laundering (AML) as their single top issue compared with non-financials such as corporates and professional services firms who face a wider set of issues and are more worried about areas like talent acquisition and workforce management, and cybersecurity threats.

TOP CHALLENGE – BY SECTOR



With the growing complexity and stringency of modern compliance rules, it is understandable that teams in both financial and non-financial industries see this as their top concern, with 27% of financial services companies and 19% of non-financial entities citing this. As new rules require lower tiers of the supply chain to be scrutinized, or owners with smaller percentage stakes, this adds to the workload of risk and compliance teams.

As a much broader cohort, featuring highly regulated industries (like pharmaceuticals and energy) and non-regulated industries (like retail), the non-financial sectors have a far less harmonized regulatory framework. Depending on the sector and its size, these can encompass various regulations, such as AML/CFT, Anti-Corruption, and Corporate Sustainability Due Diligence (CSDD), but can also by very light touch and less complex in comparison. Accordingly, it's understandable that compliance complexity doesn't feature as high for some in the non-financials group.

Economic volatility and financial risks are a feature of a global system where businesses are connected and interdependent. Companies rely on a network of third-party providers and vendors. Understanding who is in your supply chain – for example where raw materials originated from before they were processed – is an incredibly difficult task that people must now address. And as the world becomes more digital, this is becoming difficult. Who made each component in your product? Who is downloading your software? How can you be sure they are who they say they are?

The next highest concern is data management and quality assurance at 12% of financial services companies and 16% of non-financials. The data people are dealing with is complex, and the databases that house them come from all over the world and have a wide variety of quality and timeliness that can be substandard. Finding the right data, leveraging it adequately, keeping it up to date and ensuring it is shared widely and doesn't end up in different internal siloes is key to improving data quality for everyone.

These challenges are attracting growing attention from senior leaders as they focus on knowing who they are doing business with. We are living in an era of exponential risks, from financial to reputational non-compliance risks, ESG, and more. Leaders will increasingly see themselves exposed to dismissal and even prosecution if their company gets it wrong.

"As a general rule, a competition law breach hits your share price by 5%. A bribery allegation will take 10%, and the biggest I've ever seen is a 52% hit. What we're really interested in now is the environmental hits, the human slavery hits."

Head of Compliance, Real Estate, UK

SEEING OPPORTUNITY IN ADVERSITY

It's a difficult time for compliance and risk professionals with a long list of challenges to wrestle with, all stemming from growing compliance complexity. But at the same time, it also represents a huge opportunity for those who can get it right. For compliance and risk professionals, the place is here, the time is now.

These departments are no longer confined to the sidelines and fighting to be heard among competing voices. They are increasingly front and center, as a raft of ongoing and emerging threats and requirements make their skills essential to their organizations' success. These include:

1. Regulatory and legal compliance risks:

More stringent regulations across a growing number of jurisdictions

Introduction of key anti-bribery and corruption laws and their mandatory due diligence requirement on third parties (including the U.S. FCPA (1977), the UKBA, and France's Sapin II law), with significant implications for global business practices, and third and fourth-party risks

A requirement to scrutinize deeper layers of the supply chain (e.g., German Supply Chain Due Diligence Act)

2. Corporate governance and due diligence risks:

A need to scrutinize more and more directors and shareholders with smaller shareholdings

Increasing sophistication of bad actors to evade detection (e.g., via circular ownership and shell companies)

3. Heightened geopolitical risks:

Geopolitical tensions, and the resulting growth in increasingly complex sanctions

Heightened awareness of personal risk to board members from external risk factors

4. Technological and cyber risks:

Dramatic rise in AI-enabled fraud and cyber risks

Increase in cryptocurrency usage, with resulting increase in risk

While these factors undoubtedly create a more challenging environment for risk and compliance specialists, it elevates their profile and makes their voices heard like never before.

SECTION THREE

Spotlight on Entity Verification

WHAT'S IN A NAME?

As we've seen from the issues organizations are facing, Entity Verification is a broad subject, comprising overlapping areas. People are coming at the problem from different angles based on their organizational needs, the industries they are in, and other factors such as how sophisticated their risk and compliance functions are.

It's therefore worth defining here exactly what we mean by Entity Verification, so we are using the term consistently and people understand whether the respondents to our survey were comparing like with like, using the term frequently, and whether there was a difference between financial and non-financial sectors.

Entity Verification is the process of validating the identity and authenticity of a legal entity (business or organization) to ensure they are who they claim to be. This involves checking various documents or data against authoritative sources to confirm legitimacy.

The responses were revealing. While the term was understood by all, its usage varies widely. The term is always or frequently used by 64% of people. When you look at the sectoral split, 47% always use the term in the financial sector, while it's only 24% in the non-financial. Those using it frequently are 21% financial vs 33% non-financial.

What is perhaps more surprising is that 1 in 5 people rarely or never use the term in financial institutions, rising to over a quarter for non-financials. That can be explained by the array of terms being used to describe the data used for Entity Verification. 'Beneficial Ownership and Control' is most often used to refer to Entity Verification data at 79% of respondents. Other terms like 'Company Reference Data' (45%), 'Third-Party Reference Data' (44%) and 'Live Registry Data' (33%) also feature highly.

Interestingly the non-financial companies we spoke to also tend to use more generic terms like 'Risk Data' and 'Financial Strength Metrics' more highly than the financial sector.

It's clearly a term that tends to be used more in a regulated environment than in an unregulated one. Improving understanding and ensuring a clearer use of different but related terminology across organizations and sectors will be an important step to achieve better outcomes, share best practice, and drive a more standardized and effective approach to Entity Verification.

PUTTING IT INTO CONTEXT

It's clear from what we've covered so far that Entity Verification is used broadly by different types of organizations for many different reasons. So, we also wanted to understand its use cases, putting our data into context.

Unsurprisingly, the most common are Customer Onboarding at 78% of respondents. Perpetual KYC (ongoing Know Your Customer risk monitoring) came in at 73% and Investigations and Enhanced Due Diligence (EDD) was cited by 71%.

ENTITY VERIFICATION USE CASES

Other use cases included Third-Party Risk Management at 58% of people, as well as some more surprising uses like Sales & Marketing 19%, and Supply Chain Management at 23%. Interestingly, Supply Chain Management is significantly higher among non-financial corporates who need to monitor their supply chain for things like ESG risks on an ongoing basis.

For some companies intelligent screening is a potentially important approach where things like negative news screening on 1000s of stories each day can help flag risks regarding a supplier or customer that need to be mitigated or reported.

Also of note, while use cases like gambling or crypto currencies were at present less common, they were likely to grow in importance as digital technology continues to disrupt financial systems – opening new opportunities that also have the potential for new risks related to fraud and cyber-crime.

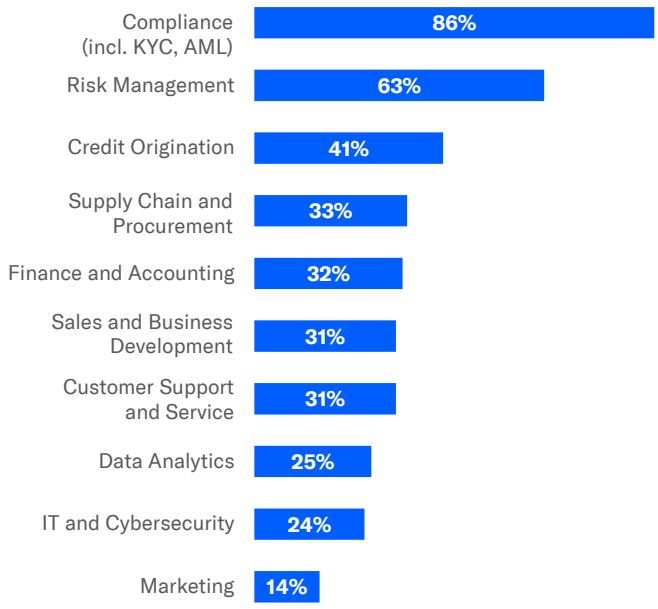
> **"My concern is with the different and growing use cases that Fintech brings. It initially was just digital assets trading on exchanges, but now it has increased to different use cases like buying a coffee or paying for your travel tickets using crypto currencies, or money transfers."**
>
> Head, Regulations and Compliance
> Fintech, Singapore

When we asked non-users of Entity Verification which use cases they could be likely to adopt, customer onboarding, KYC and due diligence featured highly, but areas like fraud prevention and supply chain management were also frequently cited – suggesting use cases will continue to change as the field develops.

DEPARTMENTS, DUTIES, AND DOMAINS

Understanding where the responsibility for Entity Verification lies and how that is likely to change in future is an important topic. Getting it right will help ensure data and intelligence is shared between departments, duplication of effort is minimized, and risks are mitigated in the most efficient way.

ENTITY VERIFICATION DEPARTMENTS OR ROLES



At present, Entity Verification is the domain of compliance and risk management, though in non-financials there is wider use by those working in finance and accounts. This balance may shift as the field becomes increasingly important to other areas of a business and its significance grows.

> **"For a long time, EV (Entity Verification) was a topic stored in the 'compliance cupboard,' so to speak. It was seen as a bit technical and not that interesting … but it's starting to come out of the cupboard and into risk management, sustainability, and other areas, as business leaders are starting to realize, in fact, that you could suffer a massive hit if you got this wrong."**
>
> Head of Compliance, Corporate, UK

The increasing profile of Entity Verification as a fundamental business function is amplifying calls within many organizations to centralize their approach. At present only 48% of respondents had a centralized approach, with 19% taking a department-by-department stance and 34% taking a hybrid approach, suggesting plenty of scope for simplification and efficiency gains.

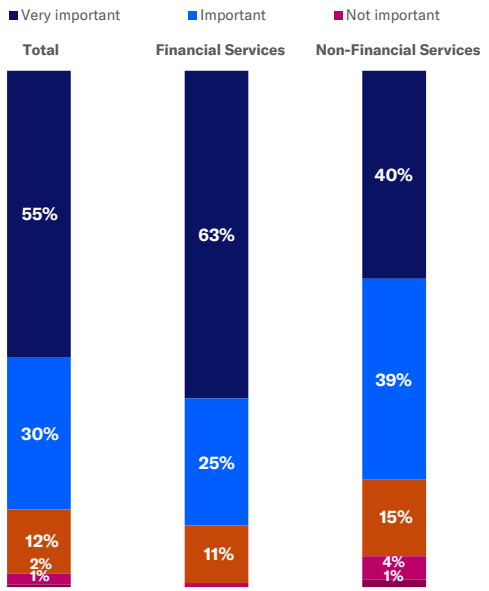
> **"We run multiple legacy ways of doing this in multiple areas of the wider business. It is expensive, inconsistent, and inefficient. We want to take a more centralized approach to improve these things and save time and effort."**
>
> Chief Data Officer, Banking, UK

> **"Our organization is maturing into a more risk-aware culture. Entity Verification is a component of that, and we are moving towards more centralization of that function over the next 12-18 months."**
>
> Head of Financial Crimes, Professional Services, USA

This centralization is one way to ensure a consistent approach to how data is harvested, managed, and leveraged. That can sometimes mean taking away some of the tools departments are using, which requires a significant culture change.

Timestamping of data, for example, was a relevant illustration of this. It involves understanding when data was collected, by whom, the timeliness of data, when it was acted upon last or passed on to clients, or third parties. Having full information on data lineage as well as a clear audit trail is a fundamental need and one that is far easier to achieve when operations are centralized and performed by a single team.

IMPORTANCE OF HAVING REGISTRY DATA TIME-STAMPED



As we can see, timestamping of primary source entity data is very important for 55% of all respondents and important to 30%. And when you look at Financial Services more people identify it as very important, reflecting the highly regulated nature of business in this sector. The requirement to base Entity Verification on real-time entity data coming from primary sources, with a full audit trail outlining when the data was pulled from which source, is becoming increasingly important across regions.

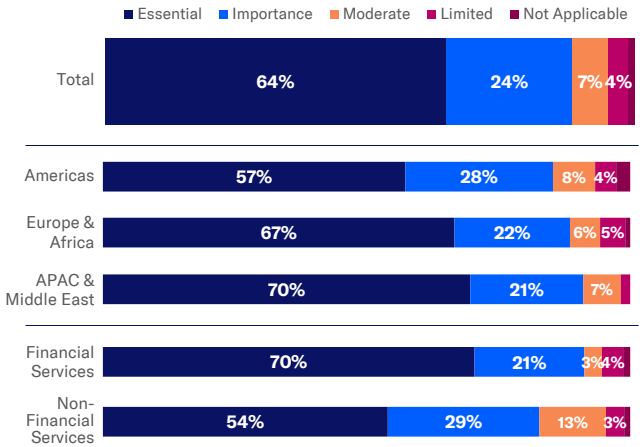
> **"I need metadata for when documentation was updated in our system, when it was updated in the parent system, when Companies House got it, when our data provider got it, and when the client got it. I need a full trail from start to finish of that document. I need to understand that I'm using fresh and up-to-date data that is within the timelines of what the client is requesting."**
>
> Compliance Director, Professional Services, USA

THE IMPORTANCE OF ENTITY VERIFICATION

> **"Entity Verification is the absolute bedrock of everything a bank does."**
>
> Head of Financial Crime Investigations, Banking, France

As the above quote suggests, Entity Verification is of vital importance to many organizations dealing with risk and compliance associated with third parties. In fact, 90% of respondents told us that it's essential or important (64% essential, 24% important).

IMPORTANCE OF ENTITY VERIFICATION



Within financial services, that rises to 70% ranking it as essential and 21% important. Even in non-financial sectors, only 16% of people were saying it was of moderate or limited importance.

It's unsurprising given the increased scrutiny on the need for effective Entity Verification. Senior management are beginning to recognize the heightened risks and complexity in the compliance world and the need to demonstrate an elevated level of due diligence to regulators. Entity Verification provides the solid foundation for compliance. And as the quote above states it is the bedrock, without which the rest of screening and compliance are potentially going to faulter.

So, when we asked people if they saw the importance of Entity Verification changing, almost everyone said it would remain stable (27%) or increase in importance (73%), with no one surveyed thinking its importance would decrease in the next two years. In financial services up to 79% believe it will grow in importance.

MAPPING THE MOTIVATIONS

What is driving organizations to prioritize Entity Verification? As we saw at the start of this paper, companies face a growing set of challenges and complexities in the risk and compliance landscape and the move towards Entity Verification is being driven by these factors. From Enhancing Risk Management and Due Diligence (86%) to Evolving Regulatory Requirements (72%), Improving Customer Identification and the Ultimate Beneficial Owners (UBOs) (71%), or Improving Due Diligence (70%), the top responses driving the focus on Entity Verification should all feel familiar.

More creative uses of data like Enhancing Marketing Quality (11%) or Improving Customer Experience (31%) rank further down the scale.

And when we look between financial and non-financial sectors, some clear themes and differences become apparent.

Among financial services respondents, there is a recognition of Entity Verification as a precondition for other risk screening activities. There is the pressure to meet ever-more stringent regulations, as well as a desire to increase automation which demands financial entities know exactly who they are dealing with before letting a computer handle the more process-driven side of things. Banks also cite a desire to improve customer experience and streamline onboarding, with specific regions (e.g., East Asia, Africa) noting this as challenging.

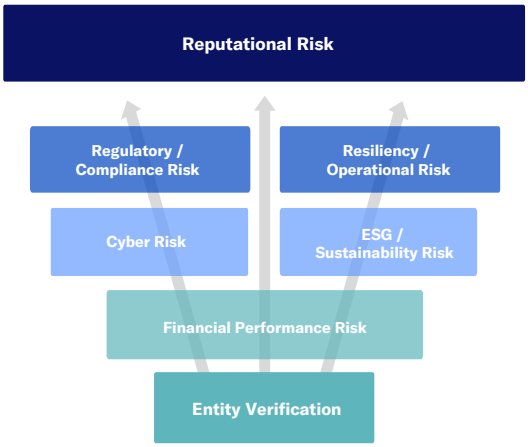
> **"In my opinion, for the overall success of compliance related work any organization takes for its clients or businesses, Entity Verification is the number one priority. Also, to keep up with required AML and CTF policies and procedures this for sure plays a vital role."**
>
> Head, Regulations and Compliance, Fintech, India

Among non-financial services respondents, Corporates are quick to flag supply chain complexity, and the risks from bad actors who are becoming ever more sophisticated. There's also a heightened awareness of Entity Verification as part of a wider risk framework among unregulated companies. And finally, Professional Services cite the additional factor of wanting to demonstrate risk robustness as part of their wider appeal to customers.

> **"Put simply, we need to make sure that those whom we are transacting with are not involved in any business we deem inappropriate."**
>
> VP, Third-Party Risk Mgt. Corporates, USA

LAYING A STRONG FOUNDATION

From what we have seen and heard, far from being another step in the risk and compliance process, Entity Verification should be viewed as the foundation upon which other processes are built.



Without effective Entity Verification, it's impossible to know with certainty you are evaluating the legitimacy and trustworthiness of the right company and its related entities. You cannot know if you're looking in the right place along a supply chain for ESG and sustainability risks or know you are protecting yourself from cyber threats. These issues can leave organizations exposed to operational risks like bad debts or loss of customers, and more importantly, it opens the threat of falling foul of AML/KYC regulations with non-compliance risks. At the top of the ladder, companies' reputations are on the line. In a digitally connected world, when bad news travels fast, reputations are what businesses live and die by. And protection from reputational risk can begin with Entity Verification.

"A recent Harvard article that said a CEO of a major corporation is more likely to be fired for an ESG-related issue than for a failing to meet financial targets. It's becoming more and more important to understand who you're dealing with and what they really are."

Head of Compliance, Real Estate, UK

For many risk and compliance professionals, these challenges provide a real opportunity to elevate their organization's approach to Entity Verification and KYC more broadly and get internal traction and attention for their work. It's a process that is vital in today's world of exponential risk and growing compliance complexity. And it's one that needs continual renewed attention from onboarding to ongoing monitoring as compliance and risk functions face dynamic challenges in a rapidly changing environment.

SECTION FOUR

The devil is in the data

DATA MATURITY

Getting into the details of the issue, the ability to verify the details of any entity ultimately depends on the information and data that is sourced. Consequently, it's important to look at data maturity and data governance when considering how well organizations will perform.

The results are telling, with nearly two out of three describing their data as 'Inconsistent' or 'Fragmented'. In other words, 62% see their data as low quality.

DATA MATURITY

With only 16% of companies rating their data as superior or high quality, there is significant progress to be made. A huge 84% see significant limitations in their data.

When we break it down between sectors, more than 1 in 4 in financial services companies see their data as fragmented, with 35% describing it as inconsistent.

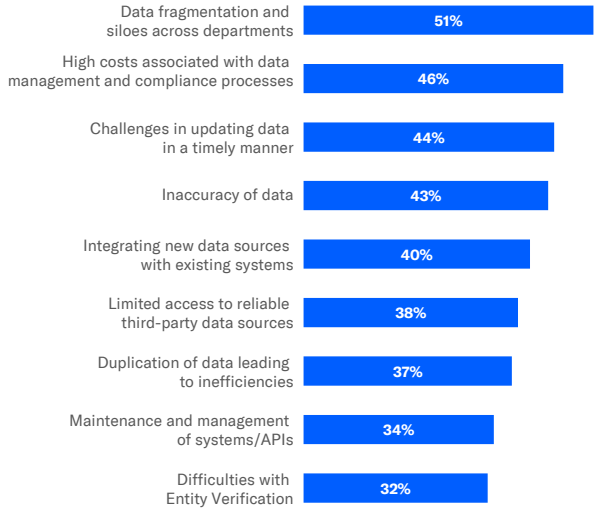
> **"I think most companies don't think enough about their data systems. They've just got used to them and don't think about what more insights the base data can provide about what they're doing, to make them more efficient and avoid duplication."**
>
> Head of Compliance, Corporates, UK

RUNNING THE NUMBERS

When it comes to explaining why, companies face a myriad of data challenges. Data fragmentation and siloes across departments tops the list at 51%.

High costs at 46%; challenges in keeping data up to date in a timely manner, 44%; inaccuracy of data 43%; and integrating new data sources with legacy systems 40% – all feature high on the list of challenges.

DATA MATURITY CHALLENGES



And the data picture is changing all the time, often for the better as new technologies improve the quality and accuracy of information available. But with so much data out there in the world, dealing with vast amounts of information, having to check its accuracy, and dealing with countless sources of widely varying quality needs constant attention, which is time consuming, even for the biggest companies.

Dealing with fragmentation between different business areas is important to improve data maturity across organizations and ensuring that data harvested in one part of the business, like onboarding, is made available to others, like Enhanced Due Diligence.

> **"Lots of data is fragmented and that's to do with the organization. Onboarding is owned by one area, then EDD is another area. So, it's making sure that those dots are all joined. Really it needs to be in machine readable format if we really want to get things joined up."**
>
> Compliance Manager,
> Credit Management, Sweden

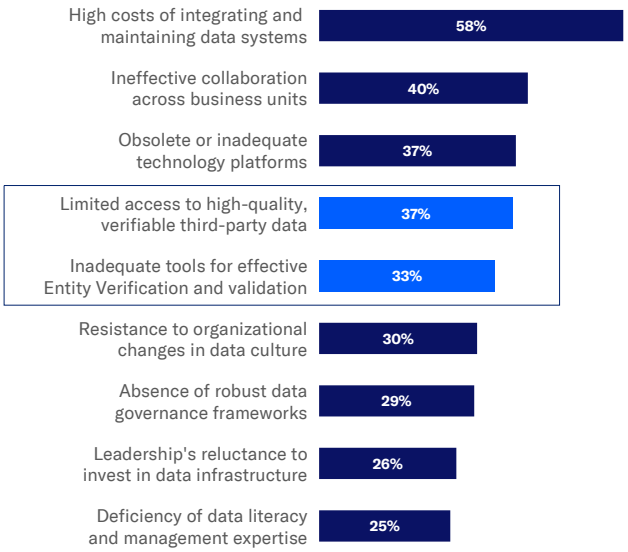
WHAT'S IMPEDING PROGRESS?

There is widespread recognition of the detrimental impacts of poor data maturity. These include compliance risks and potential penalties which 62% of people mentioned. Also at 62% were operational inefficiencies and higher cost. And challenges in Entity Verification leading to missed KYC/AML issues was cited by 60% of respondents.

What's stopping companies from addressing these well-known issues? Well, concerns about high costs understandably top the list with 58% of people feeling this is a barrier to reaching data maturity.

Given these systems' primary function is to protect against losses rather than generate revenue, proving the value of investments is difficult, particularly when budgets are already stretched.

BARRIERS TO REACHING DATA MATURITY



Ineffective collaboration and the data fragmentation we just spoke of are another barrier to effective data maturity – cited by 40% of people. Data fragmentation includes the challenge of reconciling multiple external vendors' data with internal records.

Then platform challenges and obsolete or inadequate technology (37%) is another widely reported problem impeding access to high-quality data and adequate screening tools.

THIRD-PARTY PROBLEMS

There is also a large degree of dissatisfaction with many of the tools used for Entity Verification, due to poor third-party data quality (37%) and inadequate solutions for effective Entity Verification and validation (33%).

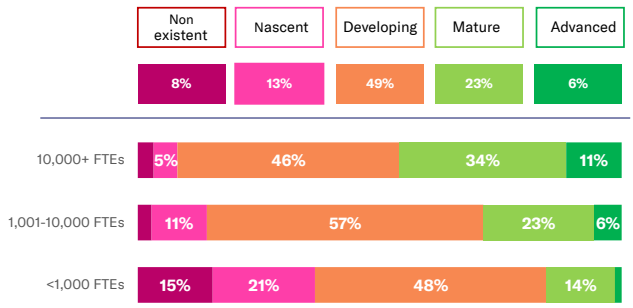
These issues stem from a reliance on multiple technologies which face integration issues, particularly combining multiple external data sources into internal tools. Systems and data in one country may be vastly better or worse than in another, this provides incompatible information or leaves gaps in the Entity Verification process.

Even internally, transparency of data can be poor with information on the same entity held in multiple places. And obviously the cost of accessing the right databases and systems can be prohibitive to progress, particularly for small organizations.

TOWARDS ENHANCED DATA GOVERNANCE

It's clear governance problems are at the heart of issues many organizations are facing with their data. Many people we spoke to talked about having robust frameworks and strategies in place to dictate how data was dealt with. The problem lay in ensuring those frameworks were followed. With a raft of systems to navigate (some of them outdated) and different teams logging information, ensuring data is recorded accurately and in a timely manner is a challenge. Data governance is clearly a work in progress, with fewer than 1 in 10 firms describing themselves as 'advanced' in data governance, with most in the 'developing' phase.

DATA GOVERNANCE MATURITY: BY COMPANY SIZE



As the chart shows, size matters. Larger companies rate their governance better, with 45% viewing it as 'Mature' or 'Advanced'. That compares with only 15% in small companies and 29% as an average across companies of all sizes.

> **"Even though we have data governance in place for new data, we still have a whole bunch of legacy suppliers we need to work on. It's not tied together. We can't see it end-to-end. We have different teams that work inside those protecting each of the areas."**
>
> Global Head - Risk & Compliance, Corporate, USA

The organizations that are leading the way in data governance are more likely to have a Chief Data Officer in place. And they are also more likely to make it a priority for discussion at board level, with 50% of companies with advanced or mature data governance making this a top priority vs. only 22% of those who rate their governance as developing or worse. Put simply, when it is a priority at board level, data governance is more likely to improve and be mature or advanced. And when you look at the benefit that delivers, clear robust data governance is a target to strive for.

BENEFITS REALIZED FROM DATA GOVERNANCE STRATEGY: TOP 6

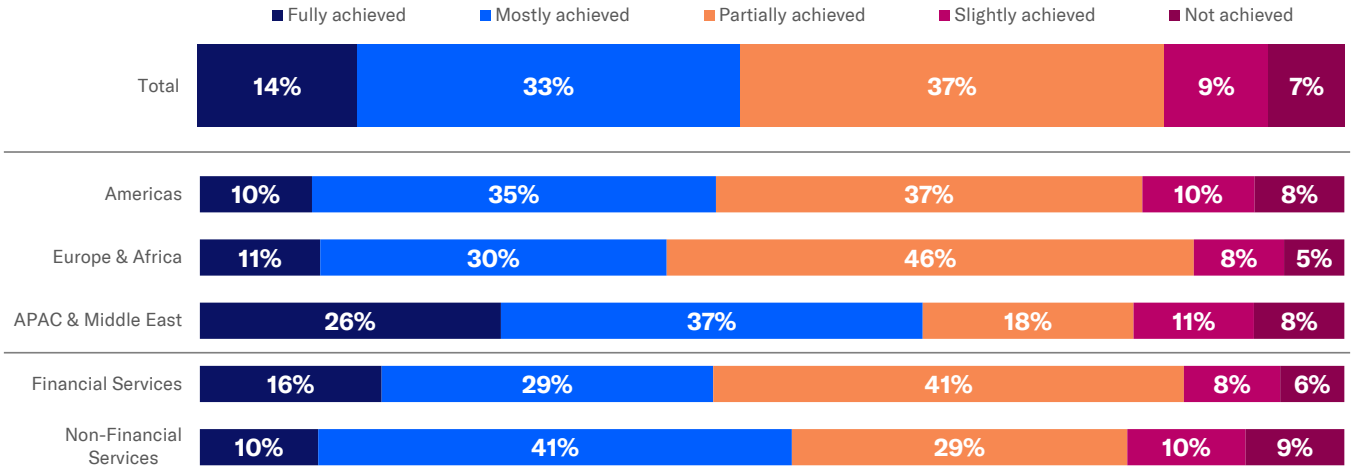
Improved data quality and accuracy	82%
Strengthened risk management and security measures	72%
Enhanced operational efficiency and reduced costs	70%
Facilitated compliance with existing and new regulations	69%
Reduced fragmentation of data among organizational siloes	62%
Provides holistic view of clients and / or third parties	58%

SECTION FIVE

The elusive goal: a single customer view

Given the vast problems people face with competing systems and data fragmentation, moving towards a single customer view of each entity seems like the ideal level of data maturity all companies should work towards. But is that realistic or even achievable? Would the costs outweigh the benefits? And how far along that road do people currently see themselves?

TO WHAT EXTENT HAVE YOU ACHIEVED A SINGLE CUSTOMER/COUNTERPARTY VIEW



Only a small minority of respondents have fully achieved a single customer view at 14% – mostly top-tier banks and small fintechs. Over half claim to be some way from this goal. When we look at different regions, APAC and the Middle East are performing best, with 66% 'Mostly' or 'Fully' achieved. Europe and Africa lag at only 41% in this bracket, reflecting a less mature approach to data and perhaps a reliance on multiple third-party databases.

Financial services also trail non-financials, which is reflective of the more stringent compliance requirements in the sector, causing businesses to rely on multiple sources of data, as well as a continued dependence on outdated legacy systems created in the early days of AML and KYC.

LEADING THE WAY

What makes leading companies different? Well, the companies that are more advanced in their progress towards a single customer view have implemented a wider range of measures including establishing a data governance framework (reported by 56% of those with a fully achieved single customer view) and engaging in ongoing staff training (56%).

There is also a strong correlation with data governance among firms reporting the strongest single customer view. Two thirds have advanced data governance and Master Data Management (MDM) with more centralized budgets for achieving a single customer view. Clearly those businesses who invest in the data governance strategies we just spoke of are closer to reaching a single customer view - one enables the other. Conversely, three quarters of those with limited single customer view have only a nascent or non-existent data governance strategy.

CASE STUDY:
MAKING A DIFFICULT CALL

A European bank we spoke to has made great advances in their Entity Verification efforts, investing significantly in creating a centralized data view and appointing a Chief Data Officer to lead these efforts. Getting senior buy-in and board level attention has unlocked investment and unified efforts towards achieving a centralized, single customer view.

But despite progress, challenges remain with data integration and GDPR compliance hurdles impeding their ability to share Entity Verification data across markets. Avoiding information siloes and achieving a single view is difficult, as legacy systems with overly manual processes hinder full automation and a positive, seamless customer experience.

Efforts continue to move towards full automation for better reliability and faster processing, but that goal remains some way off. The case highlights that even advanced banking systems face barriers to Entity Verification and obstacles in achieving seamless, centralized data management.

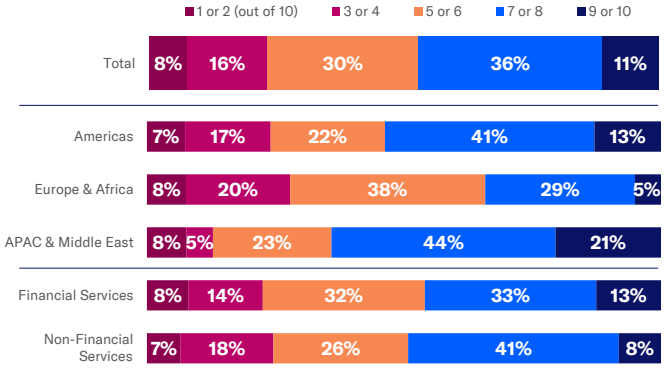
IN SEARCH OF THE 'GOLDEN RECORD'

The ultimate goal for companies involved in Entity Verification – the holy grail – is what's called the Golden Record.

The Golden Record in master data management refers to a single, accurate, and complete version of data for a specific entity. It serves as the authoritative source of truth for that data, ensuring consistency and reliability across all systems and processes.

The Golden Record helps improve data quality, decision-making, and operational efficiency.

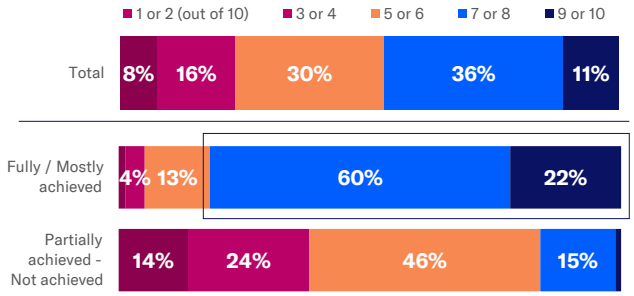
HOW CLOSE ARE YOU TO HAVING A 'GOLDEN RECORD'
(ON 1 TO 10 SCALE, 10 IS HIGH)



Only 1 in 10 firms claim to have a 'golden record', with firms in Europe & Africa claiming to be further away from this goal with only 5% of respondents stating they had achieved this. It suggests a gap in efficiency and overall compliance risk between different regions.

It also appears a two-tier system is emerging, with firms who have fully or mostly achieved a single customer view overwhelmingly closer to having a golden record. This could potentially create a performance advantage in future when compared to peers with less developed systems.

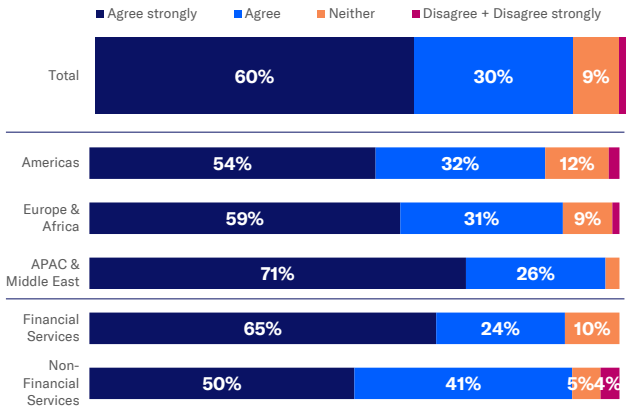
COMPANIES THAT HAVE ACHIEVED A SINGLE CUSTOMER VIEW ARE MUCH CLOSER TO HAVING A 'GOLDEN RECORD'



TOWARDS A JOINED-UP APPROACH

There is almost unanimous agreement around the interdependence of Master Data Management (MDM), Customer Lifecycle Management (CLM) processes, and KYC controls, with 9 in 10 people 'Agreeing' or 'Strongly Agreeing'.

AGREEMENT WITH STATEMENT



THREE KEY THEMES EMERGE AS TO THE INTERDEPENDENCE OF KYC, CLM AND MDM

i) the criticality of data quality and integrity;

ii) the interconnectedness and synergy between these processes;

iii) the direct impact on business outcomes when this is in place.

By understanding how MDM, CLM and KYC are intrinsically linked and working to improve each area in union will ultimately lead to superior operational efficiency, strengthened regulatory compliance, and a positive impact on customer experience.

SECTION SIX

To AI, or not to AI?

CONNECTING INTELLIGENT TECH

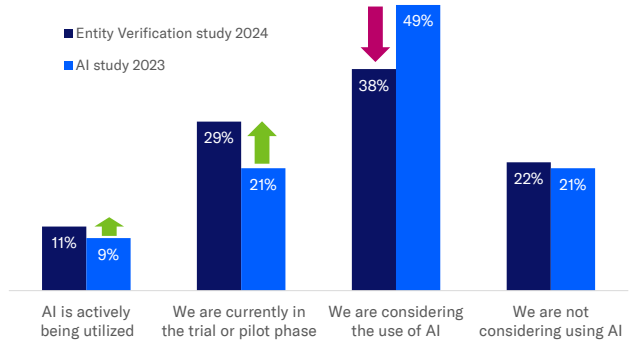
AI. You may have heard about it recently. In fact, you would have struggled to miss it. From finance to the legal profession to marketing and healthcare – if you have kept up with any tech news in the last 18 months, you will have heard that AI 'changes everything'. And it probably will. But it is not happening quite yet in this field. Because despite the hype, only a small minority (11%) of companies are actively using AI for compliance and risk management.

However, many are now in the pilot phase (29%) and others are considering its use (38%).

> **"We are in the trial phase. We are one step behind the business where it is more widely adopted among different units, due to Not being a profit center ... so any priorities with technology, innovation, go to the business first because that's where they make money."**
>
> SVP, Risk & Compliance, Corporates, Hong Kong

Perhaps what is more telling is the trend in uptake compared to a Moody's study conducted in 2023:

COMPARISON OF STUDIES



There is clearly growing use of AI for risk and compliance with more companies moving from consideration to trial and usage, while more companies are actively encouraging the use of large language models (LLMs).

As with any new technology, it is important companies are aware of the risks as much as the benefits – identifying the potential of bad actors to use these tools to subvert Entity Verification, or the multiple ways things could go wrong when they are used internally. That involves being on the front foot and exploring and trialing new and developing technology as it becomes more sophisticated.

In this endeavor, size matters. Larger companies are more likely to use or trial AI as they see opportunities to automate tasks and standardize the quality of areas like customer experience. But the trend towards AI is clear, with ongoing shifts towards acceptance, encouragement, and adoption, as more companies take a positive stance on AI, driven in large part by the rise in the use of safer, private LLMs.

ENTITY VERIFICATION AS AN ENABLER

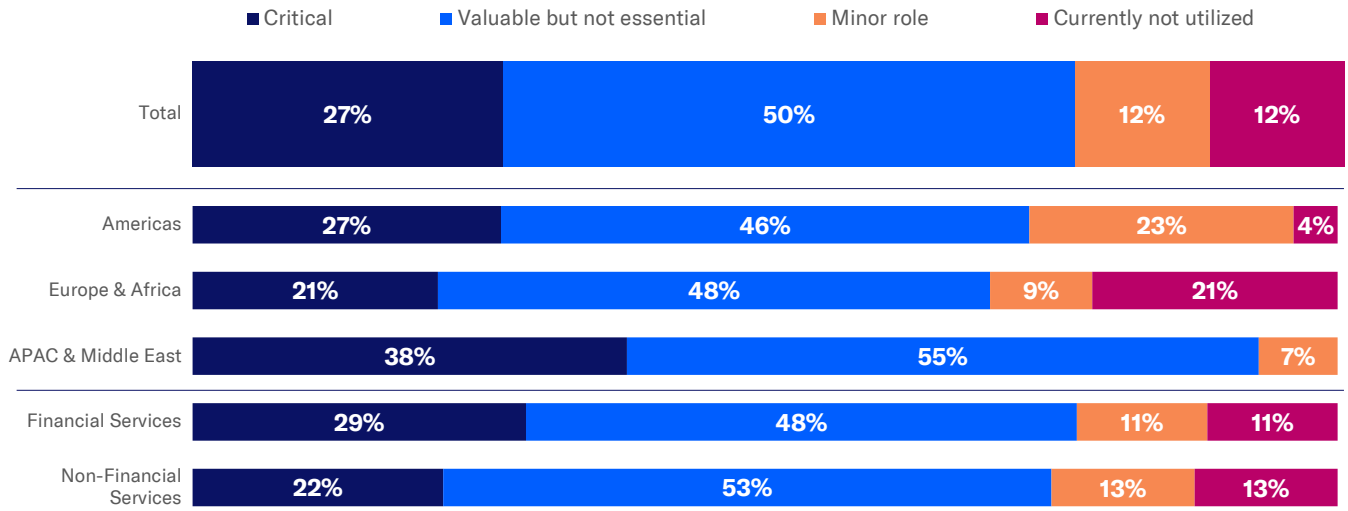
AI is coming to a risk and compliance team near you soon. But how is it going to be used with Entity Verification? Do you use Entity Verification data to enhance the data you use for AI, or do you use AI to clean the data before verifying an entity? There is a classic chicken and egg situation here.

The answer comes back to the quality of data. Good data quality is essential for effective AI adoption because AI's usefulness depends on having confidence in the data going into it.

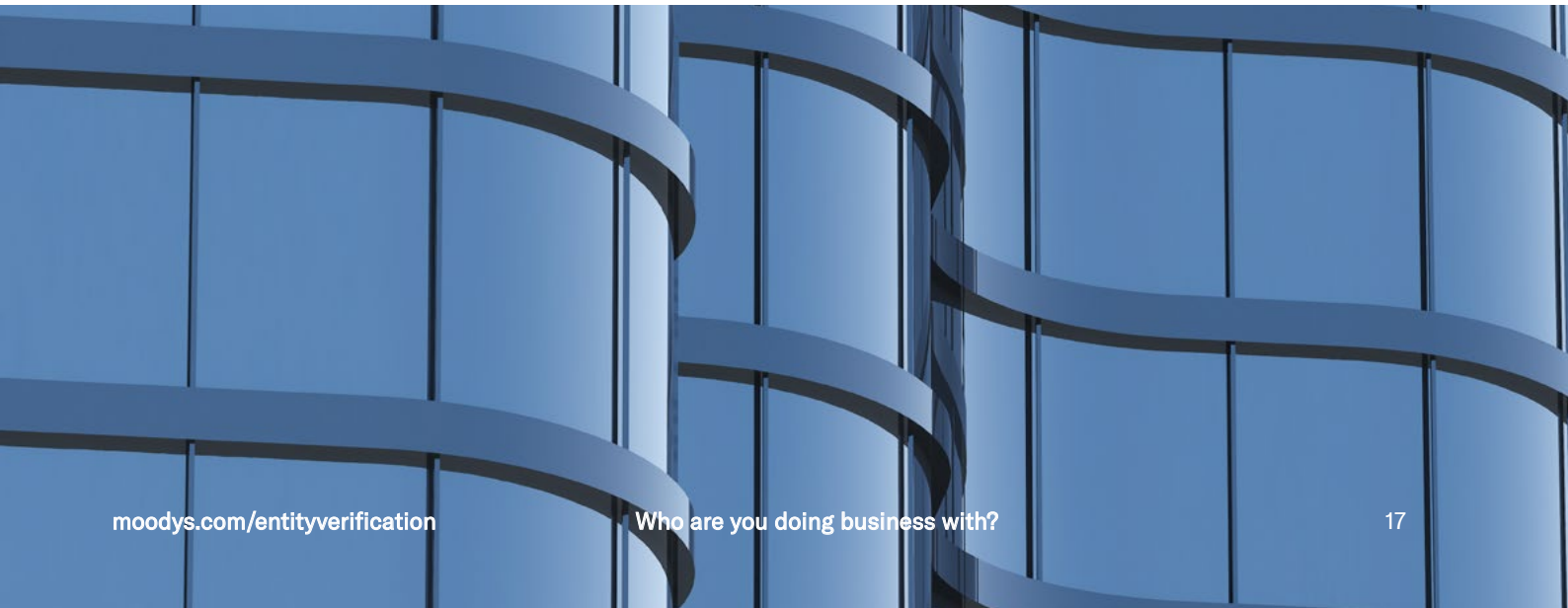
Accurate Entity Verification – and having effective Master Data Management – is a fundamental prerequisite for effective AI. And while many financial services players are trialing AI, special attention is being paid to the quality of the Entity Verification data being put into it. When you get it right, Entity Verification first enables and then enhances AI technologies.

> **"If there is garbage in, then garbage out. If I start with things that I don't trust or I can't prove, or it's making a mess, there's no way I'm going to end up with the proper compliance answer."**
>
> VP, Third-party Risk Mgt.
> Professional Services, USA

ROLE OF EV IN ENHANCING AI TECHNOLOGIES



There is broad agreement – 77% of people – on the positive role of Entity Verification in enhancing the accuracy and effectiveness of AI technologies, particularly in compliance and risk management. In APAC and the Middle East, that rises as high as 93%, again reflecting more sophisticated, technology-led approaches in this region.



SECTION NINE

Key takeaways & conclusion

As we have seen, Entity Verification has never been more relevant. From geopolitical tensions to stricter regulations and a need to get deeper into supply chains, there are many factors driving this shift. But data and organizational obstacles persist. By overcoming these challenges and others, companies can unlock better clarity in relation to the third-party entities they are dealing with, improving their risk and compliance processes across their entire organization.

01 These are highly uncertain times, with high levels of risk, but this provides risk and compliance teams with the opportunity to be heard by senior management.

02 Entity Verification is perceived as important, and is widely predicted to grow in importance; use cases are expanding as new instruments emerge (e.g., crypto).

03 Though important, EV is still more visible to risk and compliance roles, and its impact is not fully visible among the wider business and senior leadership.

04 Entity Verification needs to be considered as the essential bedrock underpinning all third-party risk management, with a direct link to the avoidance of reputational damage.

05 Data challenges include siloes, poor accuracy and the costs of remediation, as well as effective integration of internal / external data.

06 There is some dissatisfaction with the quality of tools and data for EV, not least due to the lack of clear data lineage.

07 While a single customer view is still elusive, more advanced companies are more likely to have senior buy-in, and to have implemented more measures.

08 AI and LLM (Large Language Model) adoption continue to progress, albeit not quickly. EV is considered by many as the key to unlocking AI, by ensuring data accuracy.

As digital technology continues to develop, companies must ensure they are positioned to seize the opportunities it presents. Ensuring they have access to high quality data, good levels of data maturity, and data governance unlocks the door to effective Entity Verification, which in turn, enables the use of AI in this sphere.

And as we learned from our research, good Entity Verification is the foundation on which companies can protect themselves against many other risks. It is what enables effective Master Data Management, Customer Lifecycle Management and Know Your Customer activities.

When you see it in this light, it couldn't be more important. Those companies that can overcome these challenges will be best placed to avoid the multiple risks associated with poor Entity Verification, having a better answer to the question **"Who am I doing business with?"**

GET IN TOUCH

Contact information

Please get in touch with the team at Moody's to discuss Entity Verification and how to solve your risk and compliance challenges. Access real-time data from commercial registers and tax offices worldwide via our single platform for secure and seamless verification.

Visit moodys.com/entityverification for more information.

AMERICAS
+1.212.553.1653
clientservices@moodys.com

EUROPE
+44.20.7772.5454
clientservices.emea@moodys.com

ASIA (EXCLUDING JAPAN)
+852.3551.3077
clientservices.asia@moodys.com

MOODY'S