MARSH | THE LAWYER

March 2026

Law Firm Risk: Global Survey Report

Making sense of complex & interconnected risk

Contents

Introduction from Marsh	4
Methodology and introduction from The Lawyer	6
Prevailing risks in the legal sector	8
The use of Generative AI and LLMs	13
AI controls and processes	17
Anti-money laundering and counter terrorist financing	21
Cryptocurrency	26
Conclusions	29
Appendix charts	30

Introduction from Marsh

Firstly, a huge thank you to the 200 practitioners across 22 countries who contributed to this year's Law Firm Global Risk Survey. Participation at this level generates significant credibility and generates a report grounded in the realities of modern legal practice.

The past year has reinforced how interconnected risk issues in the global legal community have become. Our team has had the opportunity to present risk insights to more than 2,250 lawyers and risk professionals across EMEA, North America, the United Kingdom, and other international financial centres. Alongside this engagement, we established a dedicated client AML risk group designed to address real-world challenges faced by firms navigating evolving financial crime expectations. These conversations - practical, candid and often complex - form an important backdrop to the findings that follow.

The picture that emerges is of a profession operating worldwide in an environment where it is increasingly recognised that risk is no longer episodic but structural. It is woven into how firms grow, adopt technology, manage client relationships and respond to regulatory change. In this setting, although some have always seen risk and strategy as two sides of the same coin, risk management is increasingly perceived more widely as inseparable from strategic decision-making.

This year's survey suggests a profession recalibrating under sustained pressure from multiple directions. Traditional exposures remain present, but they now sit alongside forces reshaping the mechanics of legal practice: intensifying anti-money laundering expectations, the emergence of crypto assets (including cryptocurrency), and the rapid deployment of artificial intelligence. These are not temporary disruptions. They represent a redefinition of how firms demonstrate control, accountability and resilience while still delivering certainty and assurance to clients.

As to anti-money laundering, the survey responses indicate significant controls in place at the point of matter inception, perhaps driven by our question design. While the results are positive this raises an important complementary question: how effectively those controls continue to operate as matters evolve. The obligation to identify and respond to emerging red flags does not end at onboarding. Firms that embed continuous risk awareness throughout the lifecycle of a matter are likely to be better positioned to manage exposures before they create loss events. Next year's survey will address this point.

On the AI front, a different but equally significant governance challenge is emerging. Artificial intelligence introduces a different category of pressure. As machine-assisted tools become embedded in legal workflows, risk ownership becomes less straightforward. Decisions are no longer attributable to a single actor but emerge from an interaction between human judgement, system design and organisational controls. In this environment, the ability to evidence how decisions were reached, including supervision, documentation and traceability, becomes as important as the outcome itself.

Encouragingly, the survey shows a profession investing in internal capability. Risk awareness is broadening beyond specialist teams, with leadership engagement becoming more visible and structured. This signals an important cultural shift: risk is being recognised as a condition of sustainable growth rather than a constraint upon it.

The findings also reveal a cautious relationship with crypto asset work. Some firms remain reluctant to engage, even as regulatory frameworks and risk management tools continue to develop. While caution is understandable, prolonged lack of engagement may carry its own strategic cost. Global momentum behind digital assets, including increasing governmental engagement, institutional adoption and development of Web3 infrastructure, suggests that this is an area moving towards normalisation rather than retreat. Firms that invest early in understanding and managing these risks are better placed to participate confidently as the environment matures.

As Christine Lagarde, President of the European Central Bank, observed:

"...it would not be wise to dismiss crypto-assets; we must welcome their potential but also recognize their risks."

This balance between opportunity and restraint is increasingly becoming a defining feature of modern legal risk management.

Marsh's role continues to evolve in step with our clients. By combining claims analysis, practitioner engagement and global market insight, we aim to translate emerging patterns into practical guidance. We recognise our people must evolve too, investing in growing our human capital by engaging with AI apprenticeships and cutting-edge risk thinking to manage the emergence of novelty in what is a proliferating network of complex responsive relationships between law firms, their clients and entities who bear risk.

This report is intended to support informed choices, not simply by mapping exposures, but helping firms understand where attention and investment will have the greatest protective effect.

In a period defined by uncertainty and acceleration, resilience is becoming a differentiator. Firms that embed adaptability and disciplined execution into their operating model will be best placed to combat the uncertain future ahead. That future seems likely to remain all at once, as expected, surprising, exciting, worrying and unclear. Although the term risk management continues to occupy a very broad space, it is a great step forward that it is now seen as adding real value in navigating the unknown, rather than just being seen as optional window dressing or at worst business prevention. Whatever the future holds, Marsh is here to help on that journey.

Victoria Prescott
Senior Vice President

John Kunzler
Managing Director

Methodology and introduction from The Lawyer

This year Marsh in conjunction with The Lawyer is again publishing its annual global survey on the various risks facing the legal industry. As in 2024, 2025's research consisted of a structured questionnaire including mixed, multiple-choice and open-ended questions as well as Likert scales.

The survey was designed as a collaboration between Marsh and The Lawyer and covered several open-ended subject areas. These included key risks for law firms in 2025, AI controls and processes, generative AI and LLMs were touched on last year, whilst anti-money laundering, counter terrorist financing and cryptocurrency were new.

As in 2024 survey audiences were drawn from senior legal sector contacts from UK & Europe, North America, Central America and APAC. Senior legal sector contacts included managing partners, heads of practice, heads of risk and compliance and others focused on risk management within the firm. Demographics of respondents were analysed through firm revenue and location of respondent firms providing comparative views across different risk profiles.

Total responses to the survey were 200, an increase of 113 versus 2024's study. Survey questions were not mandatory with respondents answering questions relevant to their organisation. Base sizes of different parts of the survey therefore vary throughout the report. A full set of completed questions and base sizes can be found in the report appendix.

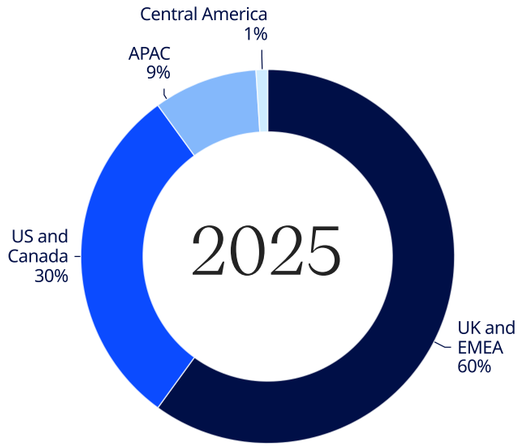
This analysis was supplemented with interviews for further context with risk leaders from UK Top 100 and US firms providing broader understanding to the key risk areas discussed. Firms had the option to provide insights anonymously or on the record as reflected in this report.

We hope you find this report insightful and useful in informing your risk approach for 2026.

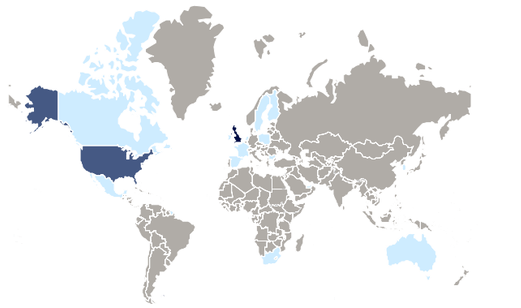
Thomas Procter
Research & Insight Director - The Lawyer

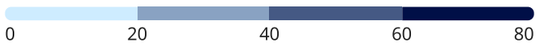
Fergus Channell
Customer Research Lead - The Lawyer

Local office by region

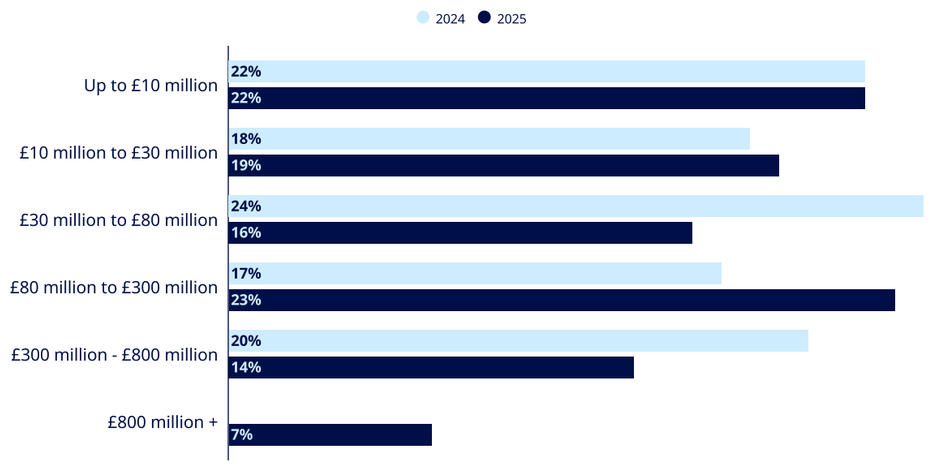


Where is your local office?



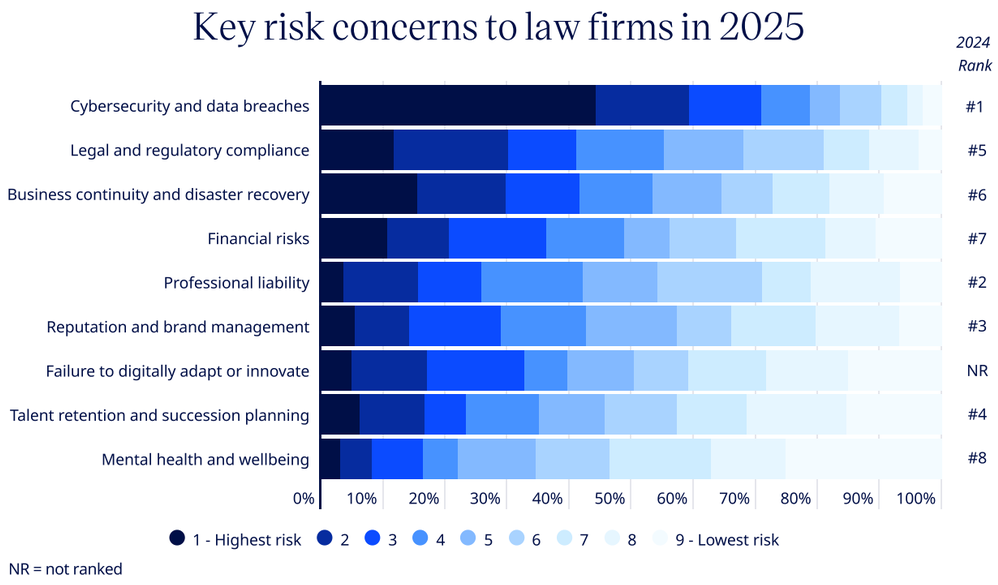


What is the approximate annual revenue of your firm (in GBP £ or equivalent)?



Prevailing risks in the legal sector

The risk landscape is constantly evolving, with risks no longer existing in isolation but rather interconnected with the capability to cause significant damage to organisations. Firms are navigating a changing number of threats and doing so through clear risk management processes, horizon scanning and by positioning risk as a key priority for leadership. As in 2024's analysis, 2025 marked another year of emerging and continued significant risks to firms. As technology use in law firms continues to advance, particularly through the increasing adoption and integration of AI, firms are experiencing new situations shaped by both internal transformation and external threats such as cybercrime. The pace at which unprecedented world events are occurring has increased significantly, making future planning increasingly unpredictable, and risk mitigation ever more difficult. Firms are not only preparing for existing risks but also building resilience to the unpredictability of the global landscape and the now commonplace extent of geopolitical volatility.



Risk management is, therefore, challenged to deliver an effective risk approach to tackle the unknown. As explained by Alex Ktorides, Head of Risk and Compliance at Bristows, thinking backwards from the risks most likely to do the most catastrophic damage to the firm is key. Yet what is also clear is the importance of building the capabilities to react to unpredictable risk.

Against this backdrop, firms were asked to rank their key areas of risk concern, providing a clear indication of where attention and resource are being focused in 2025.

Top-tier risks: Cybersecurity, legal and regulatory compliance, business continuity

As in 2024, cybersecurity and data protection remain the leading risk priority for firms. While no two risks exist in isolation, the potential damage to the firm from cyberattack or data breaches are considerable. Regulatory fines, reputational damage and exposure to liability are just some of the secondary implications of that exposure. In an industry where client confidentiality is key, risk of confidential data losses can have untold impact. As cybercriminals become more sophisticated in their attacks, firms must remain on the front foot in their development of new mitigation strategies and preparedness. Justin Newman, Head of Compliance & Assistant General Counsel at Gibson Dunn, explains cyber to be a large, multi-faceted risk that demands a layered approach. This includes hard controls such as perimeter fortification, prompt patching, and continuous threat monitoring, to leveraging industry-leading cloud providers for enhanced security capabilities. Newman notes however that ultimately, client data is only as secure as the weakest link, so alongside technical controls there is a necessity to prioritise extensive, tailored, and realistic scenario-based training and a multi-channel approach to ensure the firm's lawyers and staff are aware of the risks and know how to identify issues and respond appropriately by promptly involving subject matter experts.

Ranking second, legal and regulatory compliance was a key risk concern for firms in 2025. As with cybercrime and data breaches, the interconnectivity of risks and subsequent fallout helps explain this high ranking, indicating the level of concern as to how other operational failures can increase regulatory exposure. As Blake Morgan's Director of Risk and Compliance Karen Kirk explained in discussion, "risks cannot be viewed in isolation, they feed into one another with, for example, a serious data breach likely to lead to reputational damage, the risk of action by our regulators and claims from our clients". This can make the prioritisation of risks difficult and emphasises the need for an overall well-structured approach to risk management. By region, EMEA echoed the global view, ranking legal and regulatory compliance second, while respondents from APAC and North America placed lower concern in this area (but still ranked it eighth and third respectively). This perhaps reflects differing local legal responsibilities relating to AML/CTF.

Business continuity and disaster recovery ranked third, underscoring firms focus on ensuring their organisations are effectively mitigating where possible and ready to react when necessary. Whether that be stress testing existing processes, widening the ownership of risk across the organisation, or increasing staff training and understanding of risks, firms are taking numerous proactive measures to improve their preparedness. By region, respondent firms based in APAC listed business continuity and disaster recovery as a leading area of risk priority, while EMEA respondents too placed high importance on it. When split by revenue, business continuity was equally important, ranking third among firms with more than £30 million in revenue.

Mid-tier risks: Financial concerns, reputation management, professional liability

Financial concerns lead in tier two risks in 2025, ranking fourth overall. This represents a rank increase of three versus 2024. Financial risks to the firm resulting from cybercriminal and subsequent regulatory actions are significant. Professional liability ranks fifth, suggesting firms remain concerned around professional indemnity though this risk area has dropped in rank versus 2024 where it ranked third. Broken down by revenue professional liability remains an important concern among high revenue firms, ranking fourth for firms between £300 million and £800 million. In discussion with William Glynn, a Partner in the Lawyers' Liability Defence Team at Clyde & Co, he highlighted the continued importance of managing professional liability and explained that while the volume of claims against large law-firms remains broadly stable, the value of such claims and cost of defending them has seen clear increases over the last few years. William also noted a general divergence in the causes of action brought as alternative claims to negligence and a considerable increase in reports to regulators.

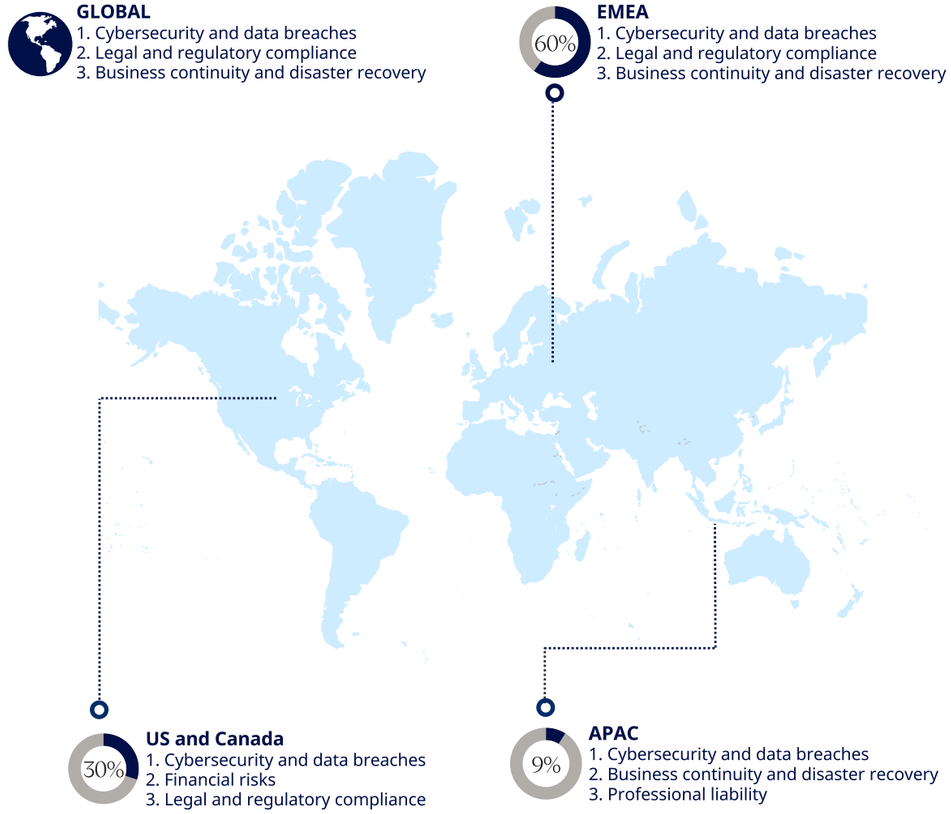
Falling 3 places from the prior year, reputation and brand management remains an important concern ranking sixth in 2025. When split by organisation size however, respondents from firms with revenues of £300 million and above placed greater emphasis on reputation and brand management, ranking it third, highlighting heightened sensitivity of larger firms to reputational risk.

Lower-tier risks: Talent, failure to digitally adapt, mental health

The areas of lowest risk concern were mental health, talent retention and failure to digitally adapt or innovate. Except for 'failure to digitally adapt or innovate' which was more mixed in perceived importance across firms of different revenue size, talent and mental health remained the lowest ranking areas of concern. Interestingly talent and succession planning ranked fourth in 2024, so

Firms are taking numerous proactive measures to improve their preparedness

Key risk concerns by region



% = per cent of respondents by location
Remaining 1 per cent of respondents from Central America

has dropped four places this year. This does not necessarily suggest reduced concern among firms in the retention of key talent, but perhaps greater concern focused on risks with greater capacity for substantial damage to the firm.

What can risk leaders take away from the above?

As in 2024, tier one risks in 2025 remain centred on events capable of causing the most significant organisational damage. Risk mitigation continues to be a central driver of decision making. Firms are placing greater emphasis on preventative controls as well as improving organisational preparedness for emerging and high impact low probability risks (HILP). Technology features prominently across these risks, both as a source of increased exposure and as an enabler of more effective risk management, with many firms responding through earlier and more consistent involvement of risk functions in strategic and operational decisions.

- Interconnected risks require greater organisational oversight. The continued prioritisation of cybersecurity, alongside heightened concern around legal and regulatory compliance, reinforces that major risk events are rarely isolated. Respondent concerns suggest an increasing awareness of how failures in one area can rapidly cascade into regulatory, financial, and reputational consequences.

- Building preventive capabilities is not just about the visible risks, but stress testing the organisation against the unexpected. The rising ranking of business continuity and disaster recovery indicates a growing recognition of the value of preparedness. Whether through enhanced training, clearer procedures, or earlier engagement with risk teams in decision making, firms in 2025 appear focused on strengthening mitigation frameworks to manage uncertainty more effectively.

Risks ranked in the mid-tier continue to reflect the importance of protecting firms from financial loss, reputational damage, and professional liability exposure. These risks are perhaps considered more as downstream consequences of failures in higher-priority areas rather than as standalone threats. Professional liability continues to represent exposure to firms though maybe less significant against the backdrop of greater risks.

- Professional liability remains a persistent exposure. While its relative ranking has declined compared to other key risk areas (probably driven by softer market conditions so cover is cheaper and more easily available), professional liability continues to represent a material concern, particularly among high revenue firms.

- Business continuity and disaster recovery's growth in risk priority, especially in EMEA and APAC reinforces the highlighted activities of building preparedness within the organisation and exploring the unlikely but potentially hugely disruptive risks to firms be it geopolitical or technological. The heightened positioning may also reflect law firms investing more widely in non-lawyer risk professionals in their risk functions.

Lower-tier risks, while still recognised as important, appear to be overshadowed by more immediate organisational threats. These include issues relating to employee wellbeing, talent retention, and the need for continued digital adaptation.

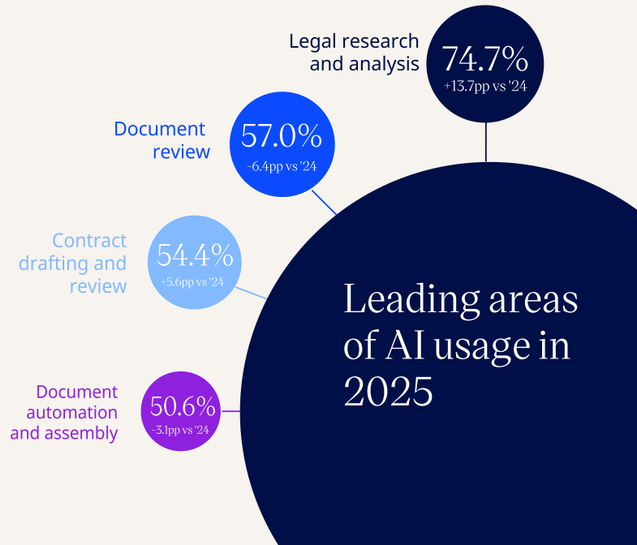
- Their positioning suggests that firms remain attentive to people and future capability risks, but that these considerations are currently secondary to managing financial, regulatory, and operational exposures.

The use of Generative AI and LLMs

Generative AI and its usage within law firms remains at the forefront of technology conversations. Firms with annual fees of less than £10 million to multiple billions are integrating AI into their workflows for productivity, potential financial gains and importantly, to stay in line with competitors. The numerous potential benefits of generative AI also create extensive potential risks to law firms. These risks can be both from inside the organisation, but also outside with tools increasing the sophistication of cybercriminal and fraudulent activity. Law firms must assess the risk both posed by external parties looking to harm their organisations and ensuring the correct usage, governance and procedures internally.

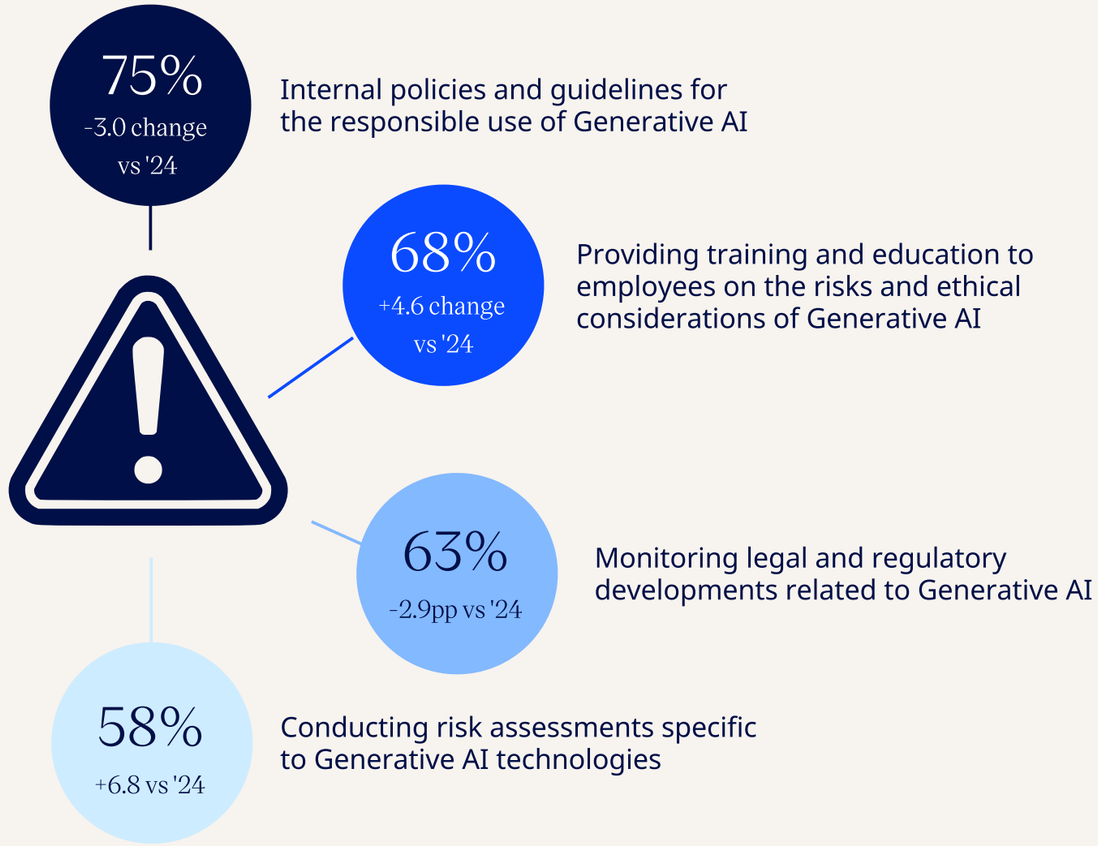
When asked how AI was currently being used by respondent law firms, as in 2024 activities such as legal research, document review and contract drafting remained high. This reflects a continued focus in legal AI usage on areas of immediate efficiency gains or historically manual, process-heavy tasks. Business development and marketing functions also saw high levels of utilisation and suggest a broadening of AI use cases beyond fee earning teams. With many firms focusing initial AI investment in fee earner teams, the broadening to the likes of business development and marketing shows firms further looking to leverage AI for efficiency and productivity gains. Respondent firms show several key gains from firm utilisation of AI, with increased efficiency, quality of work and enhanced knowledge management all areas of value. Tasks such as document review, legal research and other labour-intensive areas are therefore unsurprisingly those that have been targeted for efficiency gains. Value here can be understood not just in terms of speed and accuracy but also in the freeing of time for lawyers to spend on more high value tasks, such as servicing clients.

Widespread and increasing usage of AI tools does however present a range of risks. Multiple teams with different use cases utilising AI tools of varying degree requires a clear structured process and guardrails to ensure effective risk management. Whether it be business development, administrative or client facing legal work, ensuring clear guidance and structure around AI utilisation will help law firms protect themselves from the numerous regulatory and data breach risks that could occur in



improper use. Our research found that when asked what steps firms have implemented to address the risks associated with GenAI, emphasis was clear on the need for internal policies and guidelines, strong monitoring of legal and regulatory developments as well as training and education for employees. With AI so easily accessible and widespread, it is key that firms help staff understand the right use cases, the risks and adherence to the necessary protocols. No matter the stage firms are at in their interaction with AI, ensuring the right governance and guardrails is crucial to helping limit potential risks from misuse. Encouragingly nearly half of respondent firms had implemented at least five of the above steps to mitigate AI related risks, highlighting well-structured approaches to AI usage. In discussion with Clyde & Co Partner William Glynn, he noted the risks to law firms associated with AI to fall into distinct groupings of law firm and claimant usage. Within this William highlighted the established risks from law-firm use of AI related to hallucination, inadvertent misadvice to clients and the entering of privileged information into public AI models, with the resulting risk to confidentiality and privilege. One real risk as William emphasised was around the ambiguity of AI use in matters between client and firm. The question of risk allocation and where such risk sits, with the client or the firm was noted as having the potential to cause considerable difficulties for firms where clients insist that AI be used but where the firm remains responsible for its output. This is something that firms and clients need to discuss at an early stage of a retainer. Clients using AI to check law firm advice creates additional challenges both from a relationship perspective and in how such information has been handled, which may include clients entering privileged information into public AI programmes. William described the time and cost therefore spent in unpicking such challenges to a firm's advice as being potentially considerable. Claimant usage of AI was equally a risk noted by William, again emphasising the resource and cost related to dealing with such complaints. Complaints and claims pursued in particular by litigants in person using AI mean that Letters of Claim have grown considerably in volume and length with an often "veneer of credibility" forcing firm in-house teams to spend significant time and resource reviewing and challenging. William makes clear that no firm is immune to claimants using AI to pursue claims, irrespective as to the firm's clientele. The use of AI in claims and the risks associated is growing and not something firms can ignore.

AI risk mitigations in 2025

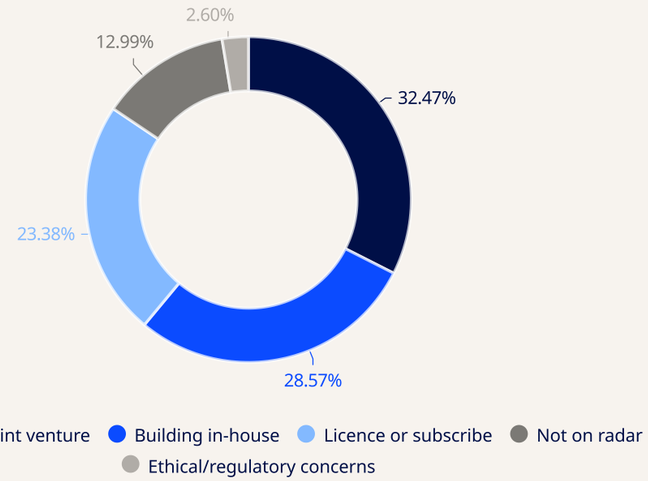


The extent to which firms are engaging with generative AI and LLMs varies across each organisation and is influenced by factors such as leadership and cultural appetite as well as financial resources. When asked whether they would consider outside investment as a means to fund AI innovation our research found the largest group of respondents were either in discussion or open to private equity backing. The remaining stated this was either not applicable or that they would not consider private equity under any circumstances. Private equity (PE) within the legal market has become an increasingly prominent topic of discussion, especially in the UK where example firms are welcoming PE-backing in the operational parts of the business, with others now fully PE-backed. With over half of respondents stating some willingness towards PE-backing in technology innovation this shows the desire of firms to stay at the forefront of legal technology and the organisational efficiencies it can provide. PE therefore creates the opportunity for firms to help drive their AI innovation and capabilities where current investment opportunity might be limited.

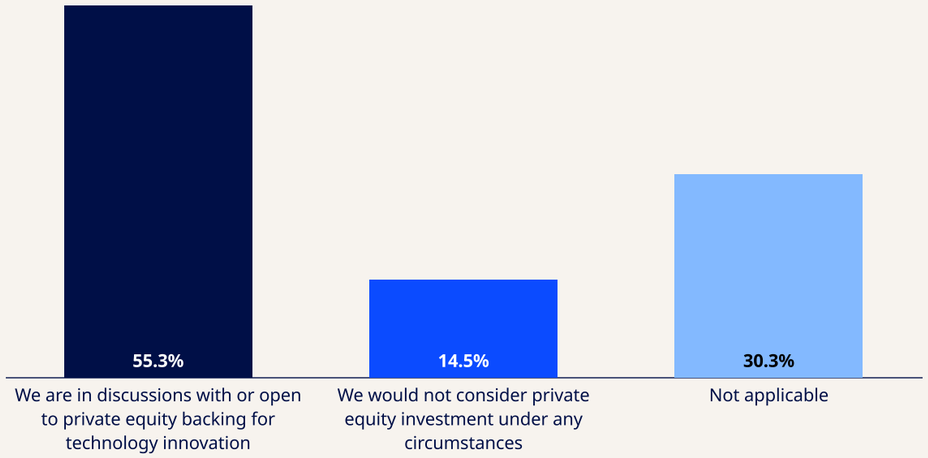
What does this tell us about law firm AI activity?

- Firms across all sizes are integrating generative AI into their processes for productivity and efficiency gains. Not doing so could have long term competitive disadvantage to firms.
- Lack of clarity around usage within law firms could create exposure to regulatory and data breaches if the correct procedures are not put in place. Firms are addressing this through clear AI policy, governance and training.
- High usage in legal research and document review shows firm desire to drive efficiency gains in time heavy processes though this should be met with caution and effective guardrails to minimise risks such as hallucinations.
- Growing deployment in business development and marketing functions implies a growing footprint of usage within law firms and further need for clear governance across legal and non-legal functions.

To what extent is your firm exploring or engaging in the development of proprietary generative AI tools?



Would private equity investment be considered as a route to fund AI innovation?

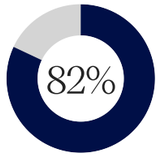


AI controls and processes

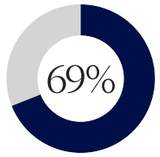
The risks related to AI usage as our research shows remain constant, with firms also taking consistent approaches to limiting risk exposure. When asked what unlawful or inappropriate AI usage might look like the usage of AI-generated content without oversight or usage of a qualified lawyer was a key area of concern. This was followed by uploading client data into public or unvetted AI tools and also generating misleading or deceptive content. The risk related to the retention of data by tool providers as well as how client data surfaces in tools is a concern highlighted in discussions with risk leaders. Submitting AI-generated content to courts was also a key area of perceived unlawful activity, and one that has been under public scrutiny. With numerous examples of AI-generated content creating false citations, precedents and cases, no firm wants their name listed against court proceedings where AI hallucinated content appeared. This reinforces the necessity of strong governance and clear training in ensuring appropriate use of these tools. As Justin Newman, Head of Compliance & Assistant General Counsel at Gibson Dunn, explains, information governance is one of the most critical risk areas relating to the adoption of generative AI tools, with the maintenance of ethical walls and other internal segmentation of sensitive information a major concern to firms and their clients. He explains how every prospective generative AI tool goes through a well-tested, multi-step assessment from initial functionality testing and security review, to evaluating tool functionalities and administrative controls, extensive piloting, and assessing residual risk before any wider rollout. Maintaining ethical walls and limiting improper use of AI tools relies both on the correct due diligence process for tools but equally on effective implementation of “hard” administrative controls, development of tailored “soft” controls (such as policies and procedures), risk-based tool deployment, and user training. As Newman notes, the firm also has a robust training programme on the appropriate usage of AI, focusing, for example, on awareness and transparency of generative AI tool usage both at the partner and associate level to promote adequate

Leading perceptions of unlawful AI usage

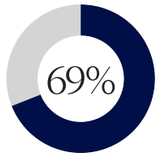
1. Using AI-generated content without oversight or validation by a qualified lawyer



2. Generating misleading or deceptive content



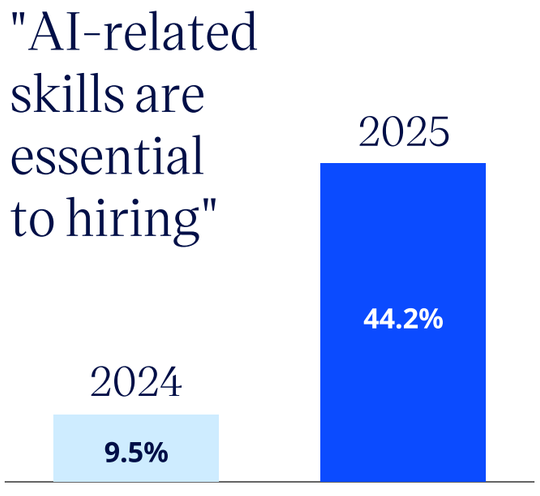
3. Uploading client data into public or unvetted AI tools



supervision, proper tool selection based on the desired use case and each AI tool's approved use cases, and, especially, the importance of adhering to local professional rules of conduct when using AI, following applicable court rules and court orders and validating generative AI output.

As usage becomes more widespread and expected in the day-to-day completion of tasks and by clients, this is also reflected in hiring specifications. Compared with 2024, the extent to which AI development has impacted the requirements for hiring new lawyers has risen considerably, suggesting the increasing importance of AI usage not just within law firms but in the skillsets, they are looking for. It also signals a cultural change occurring in firms in what is expected of lawyers. Though probably not an expectation of deep technical understanding, it does suggest a shift among firms towards increased importance in AI literacy and the ability therefore to apply more seamlessly to legal work. This shift marks a significant change to our research from 2024 when a clear majority of respondents stated core requirements remained the same. It also echoes the broader market view of AI's ever-increasing presence in the strategic agenda of firms.

"AI-related skills are essential to hiring"



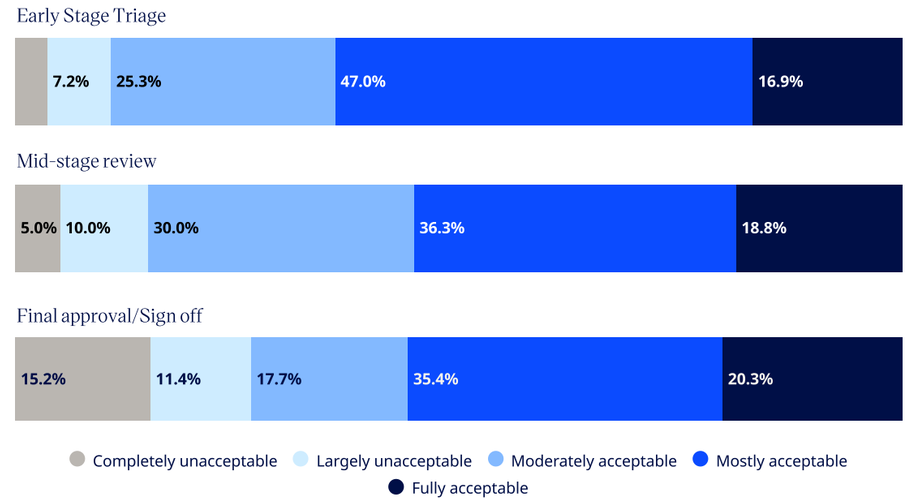
Process and governance

As part of the survey, firms were asked how they evaluate the reliability of various AI tools. The most common approach was reviewing the outcomes of internal pilot testing. Testing tools in specific areas or processes before deploying to broader parts of the business highlights a measured approach, especially when enterprise deployment of AI can involve considerable cost. Benchmarking against junior legal staff error rates is a further method of assessing AI reliability. Unless accuracy exceeds that of junior lawyers there are likely no efficiency gains in using AI. Following these two key areas, responses highlighted reliance on external consultant or vendor-provided validation data to help inform their assessments. Further market discussions highlight strong customer success from AI providers to be a valuable component for law firms as they look to best leverage their tools for specific use cases.

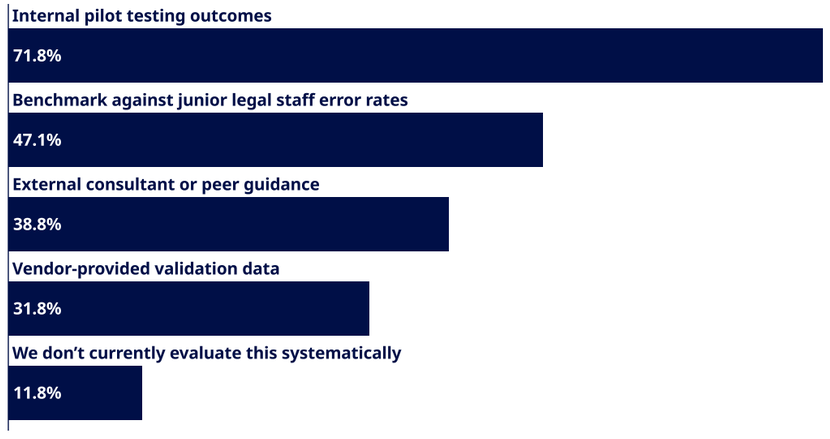
Evaluating acceptability of AI error rates against risk thresholds highlights increasing risk aversion from firms at each process stage. While AI error is more acceptable at early-stage triage, tolerance decreases as processes move toward mid-stage review and final approval. While firms are open to integrating AI into workflows, acceptance of error diminishes sharply at higher-risk stages. This reflects heightened sensitivity to risk. Overall it also showcases, in line with their risk averse nature, firms pursuing clear measured approaches.

As risk appetite decreases at successive stages of the process, the central role of risk teams in navigating and managing process risk becomes clear. For a large portion of firms, risk teams are noted to be actively involved in technology transformation and process conversations from the start. These organisations are embedding risk mitigation from the outset, understanding the potential risks of AI. When asked on their organisation's current approach to integrating risk considerations, a minimal group of respondents

How acceptable is the current AI error rate for your organisation's risk threshold at each of the following stages?



How do you currently evaluate the reliability of AI tools for in your workflow?



stated that risk was not systematically included in process design. This indicates controlled, compliance led implementations of AI and process redesign with firms. It also highlights risk tolerance is having direct influence on AI governance models.

Responses to AI and the central role of risk teams

67.1%

Risk team involvement from the outset of transformation conversations

62.2%

Risk assessment is embedded from the outset of process design

48.2%

Risk and compliance functions as one of the leading influencers on AI and legal operations redesign

As AI becomes increasingly part of the strategic agenda, the executive board is understandingly listed as the leading influence on AI and legal operation redesign decisions. The leading presence of risk teams alongside IT is also indicative of the measured risk-based approaches firms are taking in their deployment of tools, with involvement early in procurement processes. Karen Kirk, Director of Risk and Compliance at Blake Morgan makes clear the importance of having a controlled, measured approach with the risk function embedded from the start. Karen Kirk notes the use of an AI subcommittee alongside clear, consistent communication with the board as essential in creating the right governance and mitigations around AI usage.

What does this tell us about AI deployment and process design in law firms?

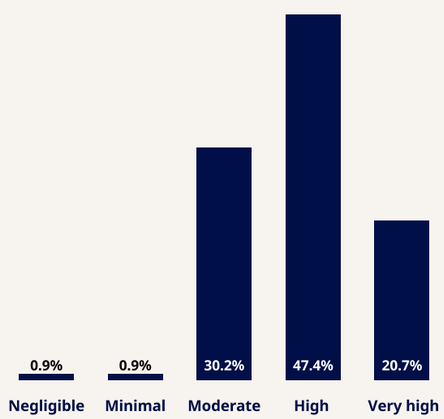
- AI rollout is often incremental. Law firms are favouring pilot-led deployment, benchmarking and staged rollout rather than firm-wide implementation both to manage costs and risks associated with AI tools.
- Risk functions are shaping AI usage in firms. With risk teams being involved from the outset, AI governance is seeing risk and compliance teams take a leading role alongside innovation. The potential benefits to firms are clear, but so too are the risks therefore requiring effective guardrails.
- Growing usage and internal evaluation of tools imply the need for widespread AI literacy within firms, with lawyers able to understand their limitations, risks and appropriate usage. Firms who are managing this effectively are creating clear structure and guidance. Creating the right environment for lawyers to leverage AI tools safely can be considered a key factor to future success.

Anti-money laundering and counter terrorist financing

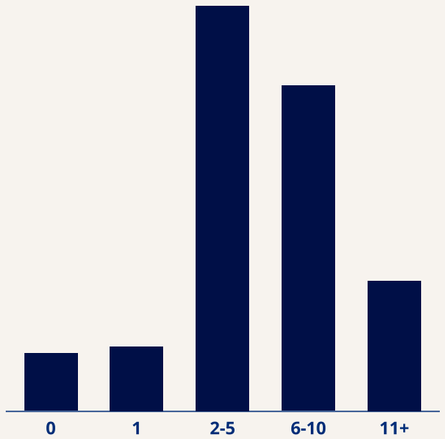
With large regulatory and reputational risks, anti-money laundering (AML) and counter terrorist financing (CTF) for many law firms is an area of significant concern. Increasingly both through strategic direction and fear of regulatory scrutiny, AML/CTF is becoming embedded as a core element of risk management for firms. AML/CTF is now framed not just as a regulatory obligation but a risk with potentially significant ramifications if not managed appropriately. As one general counsel of a UK Top 100 firm notes, it is essential to build ownership within the firm, ensuring all lawyers who are required to collect verification information are aware of the potential scale of AML related risks. For markets like the UK, the incoming takeover of supervision of AML from the SRA to the FCA reinforces the need for firms to be already proactively managing the risks associated with AML; be it through consistent staff training or increased investment in existing processes.

When asked whether their AML/CTF teams had grown in the last 12 months, overall firms noted moderate to significant increases with only a minor group stating any downsize. Firm investment in AML/CTF systems was by the majority noted as high or very high resonating with increased focus placed on AML, especially in the UK market. This sustained growth and high level of investment indicates firms responding to regulatory changes as well as increasing cross-border complexity. Growth in investment is also understood in the face of increased technology-led risks such as the sophistication of tools available to fraudulent parties. The extent to which firms are focusing or concerned on growing their AML teams is also related to the composition of work a firm undertakes.

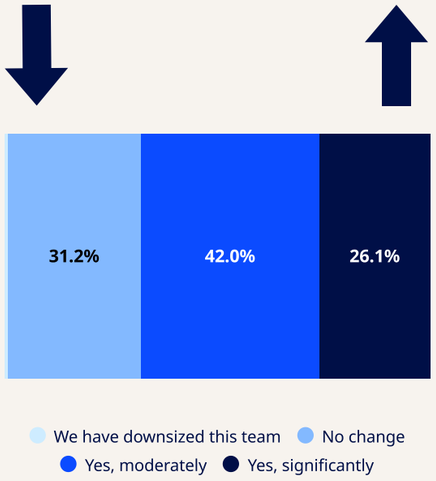
How would you rate your firm's current level of investment in AML/CTF systems and processes?



How many full time staff do you have focused on AML and CTF compliance?



Has your AML/CTF team grown in the last 12 months?

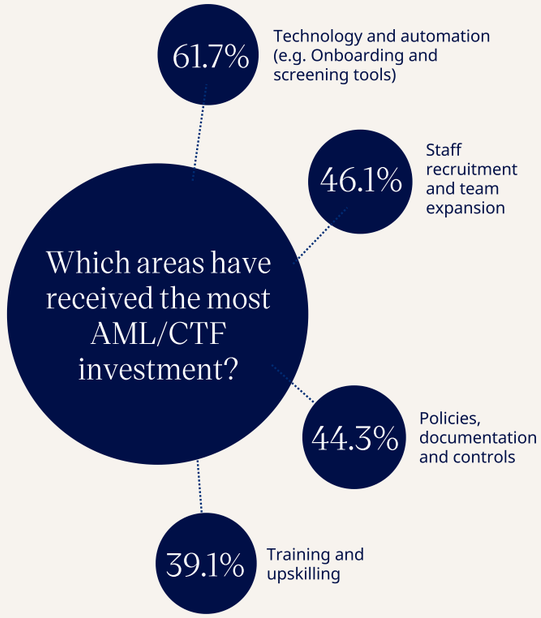


While expanding their teams, firms were overall confident in their staff to identify and escalate suspicious activity. This is indicative of effective and consistent training deployed as well as many firms highlighting a culture of general risk aversion in the organisation. As one conversation with a head of risk at a UK Top 100 firm highlighted, ensuring those dealing with onboarding and verifications are clear in what to look for and aware of the potential regulatory implications is essential. Sean Rowcliffe, Head of Risk and Compliance at Lawrence Stephens explains embedding a strong risk averse culture is key in supporting resources for AML, starting from a no and working to a yes ensures the firm takes a measured risk-led approach to AML. This highlights how building the right culture at lawyer level, like with AI usage in firms, is central to managing risk firmwide. A risk averse culture internally is also reflected in how lawyers interact with their clients, ensuring strict adherence to necessary verification and checks. These firms are making clear their stringent policies and processes for managing AML/CTF risks not only for their benefit but for their clients also.

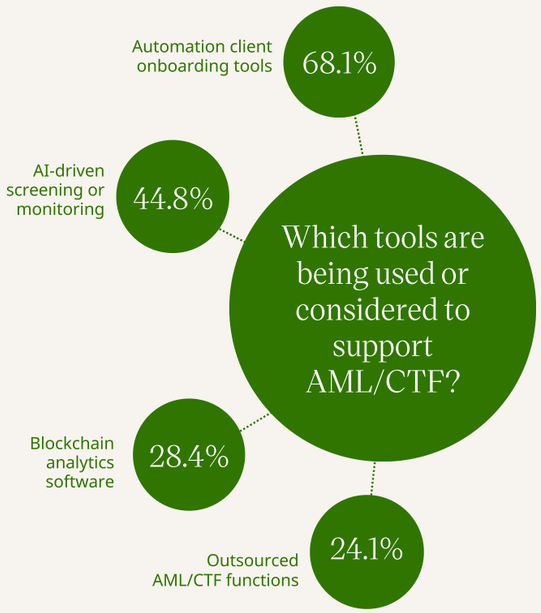
Alongside embedding a strong culture of risk awareness, firms are also pursuing improvements in process. Improved screening and onboarding tools were a key area noted by firms for AML/CTF investment, together with development of policies, documentation, controls and team expansions. This underscores firms taking a holistic approach to building out more robust capabilities, as both the regulatory obligations and the sophistication of fraudulent parties becomes more advanced.

Firms are navigating increased suspicious activity through varied means with technology playing a key role. When asked what tools were in use or being considered to support AML/CTF, automated client onboarding tools and AI-driven screening or monitoring were key areas. With the technology at fraudulent parties' disposal also more sophisticated, the use of more comprehensive screening tools beyond human checks is required.

Which areas have received the most AML/CTF investment?



Which tools are being used or considered to support AML/CTF?



One UK Top 100 firm general counsel noted that the value lies not only in reducing the time and cost associated with conducting checks in person, but also in technology enabling more rigorous and consistent scrutiny of documentation a human might overlook. There is also concern as seen with broader AI usage that tools might bypass AML processes, further requiring more sophisticated methods of identifying fraudulent behaviour. Other tools discussed include open-source banking as the quality of AI-fabricated documents increases. For firms completing KYC checks the use of AI by fraudulent actors has been suggested as a driver towards adoption of counter-AI technologies by law firms. As one UK Top 100 head of risk highlights, with AI now able to create lifelike bank statements, there is growing requirement for more enhanced verification processes.

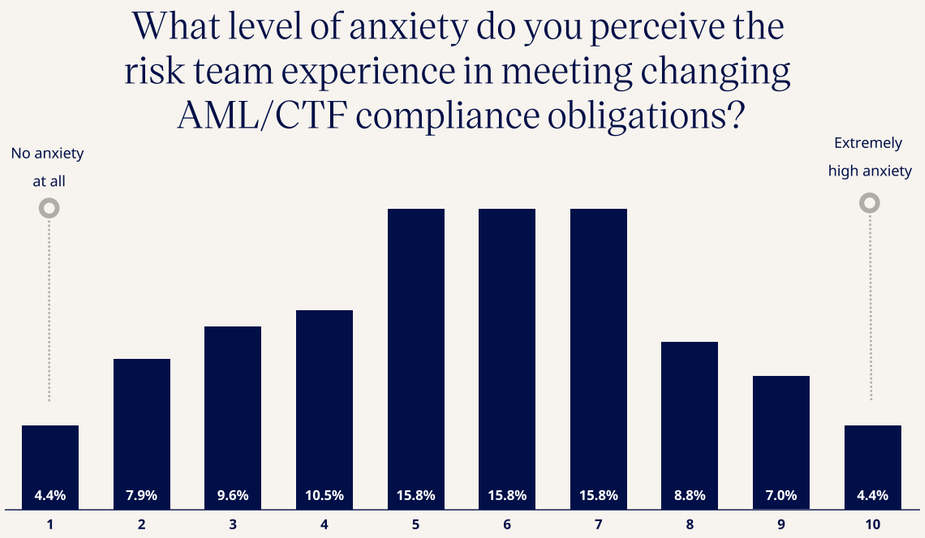
In the last 24 months have you seen an increase in the number of suspicious activities/red flags being reported?

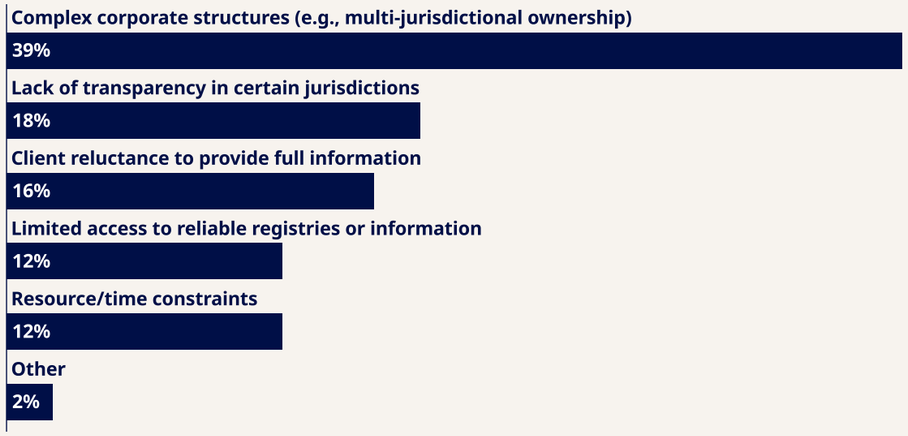
64%

Stated a slight or significant increase in the last 24 months

Our research indicates that respondent firms are taking proactive measures to improve both awareness and process for dealing with AML and CTF. While firms can be well positioned in AML and CTF processes, the ease of identifying ultimate

beneficial owners (UBOs) is also a consideration. One risk leader noted that when working with large multi-national organisations, the concern is less of fraudulent activity but rather the complication of multiple subsidiaries when dealing with transactions. Respondents when asked how challenging their firm finds it to verify UBOs of new or existing clients and counterparties highlighted an overall challenging process. This demonstrates that even where rigorous processes are in place, UBO remains complex for most respondents. As discussions with risk leaders at two UK Top 100 firms confirmed, enhanced verification from clients can have mixed reception. Large clients are understood to generally be aware of requirements and open to them, as also under regulatory scrutiny. These leaders stress the importance of rigorous upfront verification processes to support clear client communication and enable early identification of fraudulent risk, while protecting the firm.





With AI now able to create lifelike bank statements, there is growing requirement for more enhanced verification processes.

What might this mean for AML/CTF capabilities in law firms?

- Evidence suggests AML/CTF is increasingly about managing unavoidable complexity rather than eliminating risk. Firms are strengthening their teams and the sophistication of their processes to reflect this.
- Mitigating AML/CTF risk comes through confidence in staff to identify, challenge and escalate risk reflecting the importance of training, clarity of responsibility and shared awareness of the risks to both individual and the firm. This includes normalising discussions around near misses, facilitating a no-blame reporting culture and embedding risk awareness into daily practice.
- Technology is an increasingly important part of the process. As fraudulent behaviour becomes more sophisticated, firms may need to adopt increasingly robust screening and onboarding technologies.

AML/CTF is now framed not just as a regulatory obligation but a risk with potentially significant ramifications if not managed appropriately.

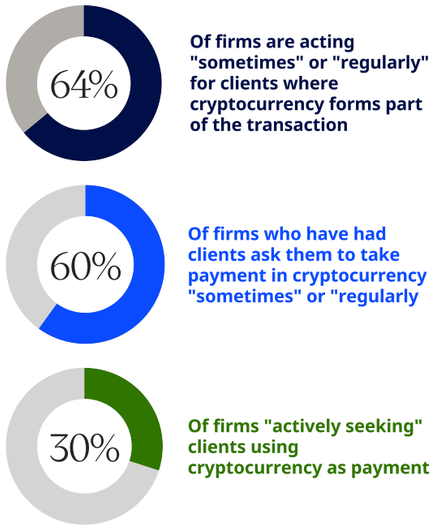
Cryptocurrency

Cryptocurrency has emerged in recent years as a common discussion point moving from the fringes to the centre of financial conversations. The associated risks and perception of it however remain varied, particularly in terms of its usage in financial transactions and the associated fraudulent risks.

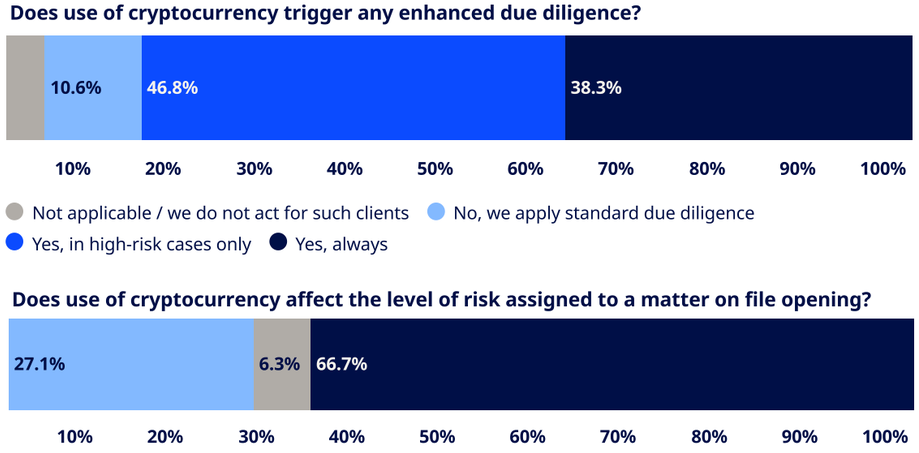
Interaction with cryptocurrency is mixed. While clients may request to transact in cryptocurrency, firms often distinguish between accepting cryptocurrency directly and accepting funds converted from cryptocurrency into currency. As one head of risk at a UK Top 100 firm explains, acceptance may take the form of converted funds rather than the cryptocurrency itself, reflecting a deliberate risk-mitigating approach.

Interaction with cryptocurrency is a further risk decision for firms. The research shows that for the majority of firms the risk level assigned to the file will always be affected by cryptocurrency. Additionally, 38% of responses stated that enhanced due diligence will be applied if cryptocurrency is involved, with an additional 47% applying it in high-risk cases. As discussions with one UK Top 100 risk leader stressed, the usage of cryptocurrency - while accepted - can activate extensive further checks to ensure a lack of criminal involvement and importantly to protect the firm from connection to fraudulent behaviour. Daniel Tannebaum, Partner and Global Anti-Financial Crime Practice Leader at Oliver Wyman similarly notes the increased diligence implications resulting from use of cryptocurrency. He explains, “as law firms expand their crypto-related business, accepting forms of crypto as tender, holding crypto assets in escrow, or engaging with crypto-focused businesses, it’s easy to underestimate the effort required to uplift the associated diligence. Given financial institutions’ treatment of crypto firms as typically higher risk, the associated diligence expectations will cascade to their clients which may include law firms in this instance”. Thorough investigation into transaction histories as well as blockchain analytics tools to validate the legal nature of cryptocurrency are some of the key methods firms are using to verify the source of crypto assets. Interaction with cryptocurrency, an area of varied response is also seen in the expertise of firms. Of those interacting with cryptocurrency,

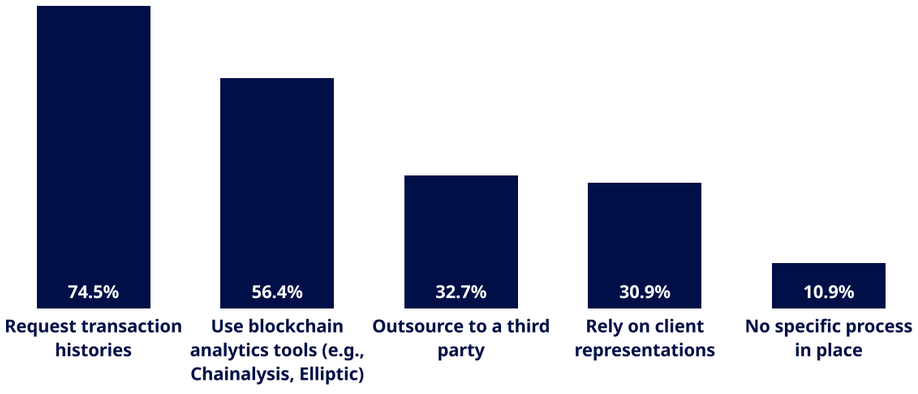
Cryptocurrency engagement and law firm risk appetite



Cryptocurrency and due diligence



Which of the following steps do you take to verify the source of crypto assets?



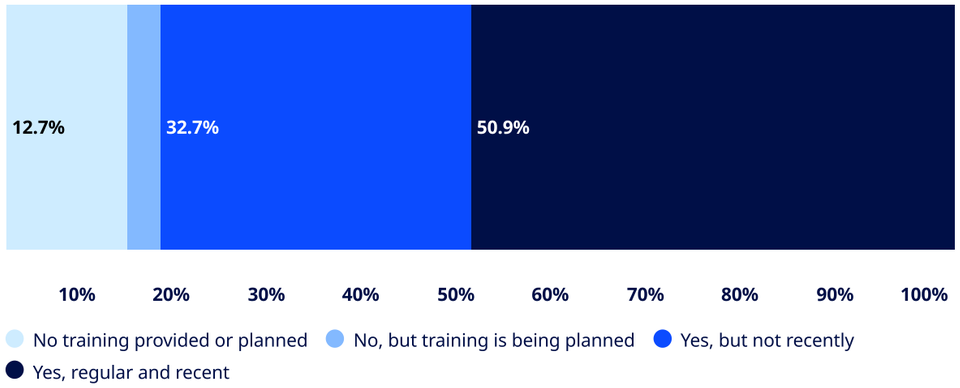
firms most commonly range between having dedicated specialist teams or specific individuals with relevant experience. This shows that firms engaging with crypto, blockchain and other digital assets are applying similar risk-based approaches as in broader AML, ensuring they have the right resources and confidence in the procedures is high.

The varied extent to which interaction with cryptocurrency is occurring however could indicate less standardisation in approach across the industry with firms operating more on a case-by-case basis. This is also seen in the lack of standardisation across jurisdictions when it comes to cryptocurrency regulation.

Considerations on interaction with cryptocurrency

- For many firms, appetite for cryptocurrency is still limited, as there remain many unknowns and the regulation of cryptocurrency is highly varied across jurisdictions.
- Where some firms are engaging and doing so with confidence, AML/CTF training and awareness building within firms is necessary to ensure adequate oversight of crypto asset risks.

Have your staff received any training on cryptocurrency-related risks?



Conclusions

2025's analysis of the global risk landscape for law firms identifies the continued concern of cybersecurity and data breaches and prioritisation of risks that have the potential to cause catastrophic damage. Risks are increasingly interconnected and being met with risk leaders thinking in increasingly un-siloed terms as to how to manage risk effectively across their organisations.

Being prepared not just for the known but for the unknown has become commonplace in the risk strategies of firms. Stress testing their organisations, building resilience and preparedness through clear process and cultural risk aversion are some of the many ways firms are managing a world of uncertainty.

The presence of AI is now widespread in firms, with many moving from pilot to wider operational deployment. Risk and compliance functions are playing central roles in influencing AI strategy as senior leadership attempt to balance innovation with risk management.

At the same time the increasing sophistication of criminal actors in their use of technology is being met with expanded AML/CTF capability, training and firm-wide awareness, supporting a more rounded and proactive approach to financial crime risk

Firms are increasingly taking a holistic approach to risk management, preparing for the unexpected and elevating risk as a key element of the strategic decision-making.

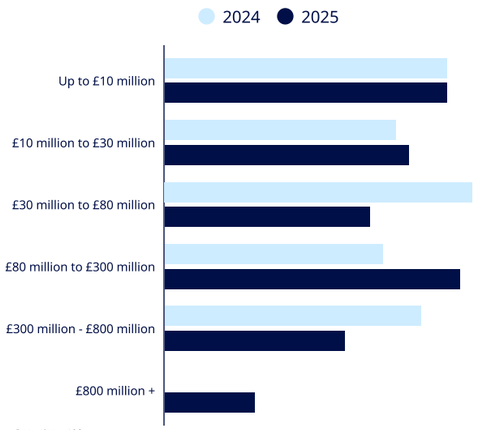
As Hilary Battison, Senior Vice President of Marsh Speciality Finpro Practice, observes:

The firms that will differentiate themselves over the next decade will not be those that avoid risk entirely, but those that understand it deeply, quantify it intelligently and govern it proactively. Risk maturity is fast becoming a competitive advantage.

Risk and compliance functions are playing central roles in influencing AI strategy as senior leadership attempt to balance innovation with risk management.

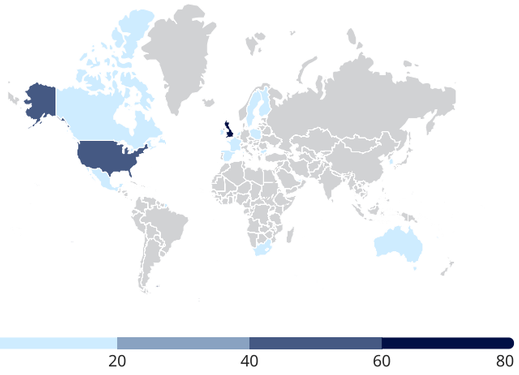
Appendix

What is the approximate annual revenue of your firm (in GBP £ or equivalent)?



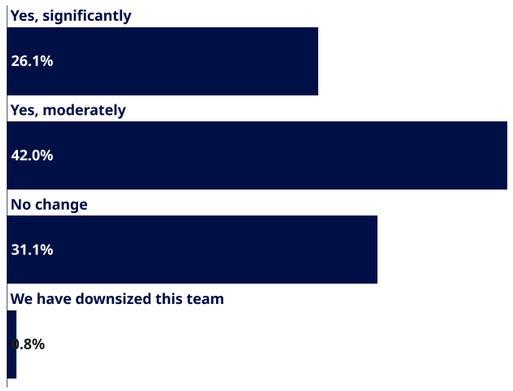
Base size = 198

Where is your local office?



Base size = 200

Has your AML/CTF team grown in the past 12 months?



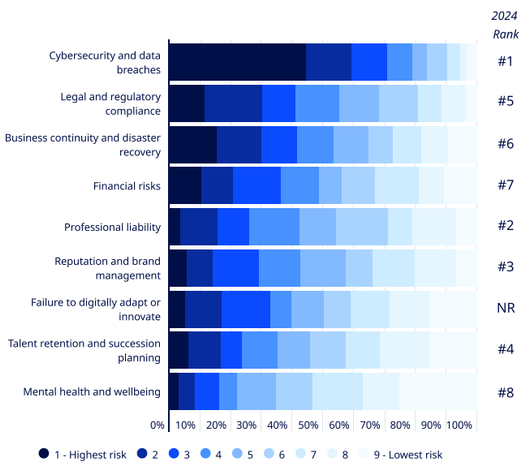
Base size = 119

How would you rate your firm's current level of investment in AML/CTF systems and resources?

Very high - Our firm has made significant, ongoing investments in state-of-the-art AML/CTF systems and specialist personnel.	20.7%
High - We have a well-developed AML/CTF framework with advanced technology, dedicated compliance officers, and clear procedures.	47.4%
Moderate - Our firm maintains baseline AML/CTF measures to meet regulatory requirements.	30.2%
Minimal - Our AML/CTF efforts are basic and reactive.	0.9%
Negligible - AML/CTF is not a current focus. There is little to no dedicated investment in systems, tools, or training.	0.9%

Base size = 116

Key risk concerns to law firms in 2025

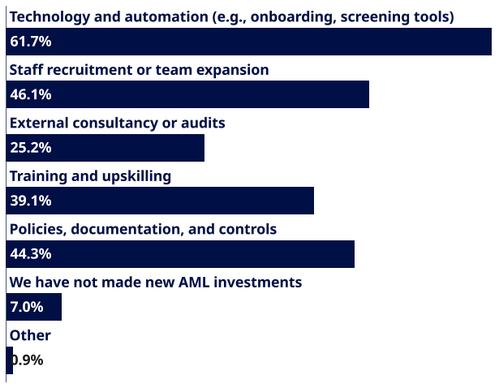


NR = not ranked

How many full-time equivalent (FTE) staff are focused primarily on AML and CTF compliance?

Base size = 121

Which areas have received the most AML/CTF investment in the past year?



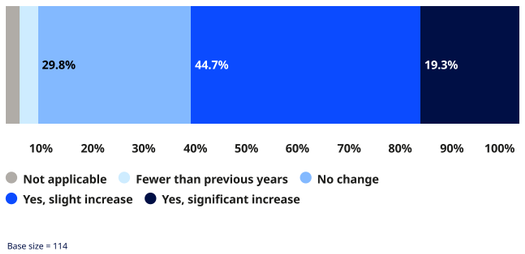
Base size = 115

How confident are you that staff can identify and escalate a suspicious activity/red flag appropriately?

Very confident - Staff are thoroughly trained and regularly updated on AML/CTF indicators and escalation protocols.	35.7%
Confident - Most staff understand how to recognise suspicious activity and know how to escalate concerns.	53.9%
Somewhat confident - There is a general awareness among staff, but knowledge varies by role or seniority.	9.6%
Not confident - Few staff are familiar with identifying suspicious activity or the correct escalation route.	0.9%

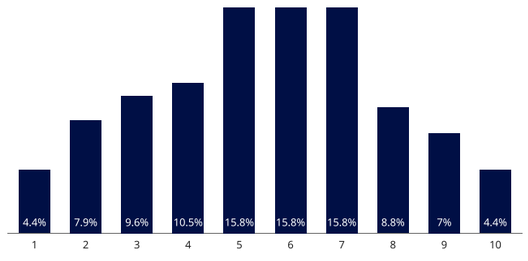
Base size = 115

In the last 24 months have you seen an increase in the number of suspicious activities/red flags being reported?



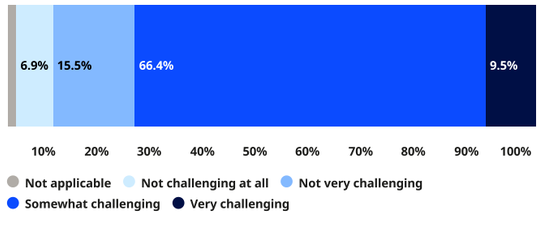
Base size = 114

What level of anxiety do you perceive the risk team experience in meeting changing AML/CTF compliance obligations?



Base size = 114

How challenging does your firm find it to verify the ultimate beneficial owners (UBOs) of new and/or existing clients of counterparties as part of AML/CTF checks and/or other corporate transparency requirements?

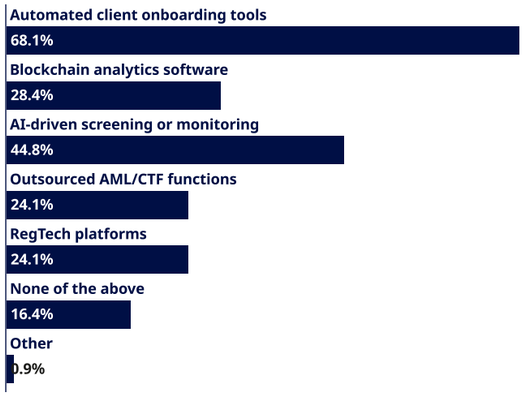


Base size = 116

Which of the following challenges does your firm most frequently encounter when attempting to identify ultimate beneficial owners (UBOs)?

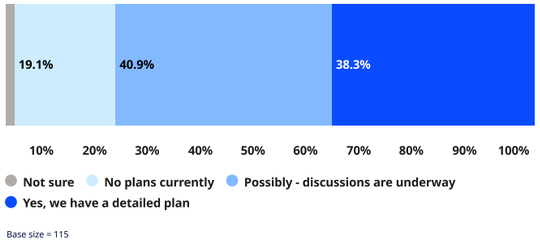
Base size = 105

Are you using, or considering using, any of the following to support AML/CTF? Please select all that apply



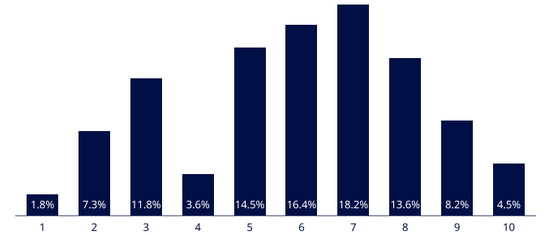
Base size = 116

Is your firm planning to expand or enhance AML/CTF capabilities in the next 12 months?



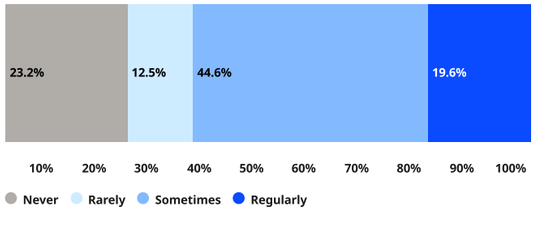
Base size = 115

On a scale of 1 to 10, to what extent have UBO identification requirements created friction with clients or caused delay in an instruction?
(Where 1= Not at all and 10 = Significantly)



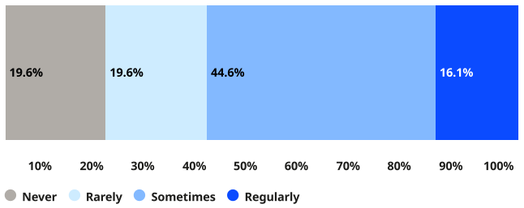
Base size = 110

How often do you act for clients where cryptocurrency forms part of transaction between parties?



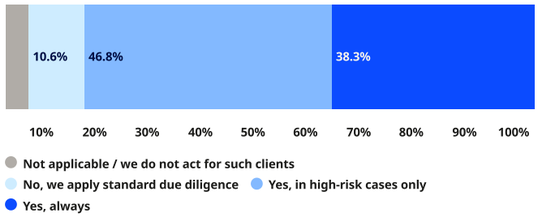
Base size = 56

How often do clients ask you to take payment in cryptocurrency?



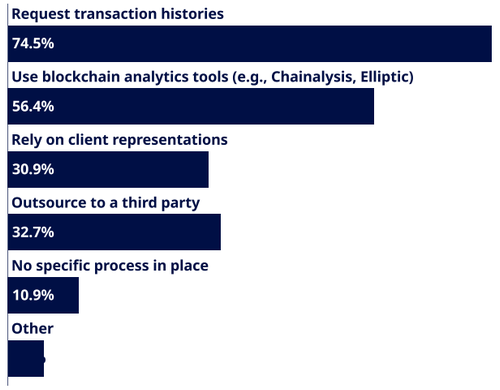
Base size = 56

Does use of cryptocurrency trigger any enhanced due diligence (EDD)?



Base size = 47

Which of the following steps do you take to verify the source of crypto assets? Please select all that apply.

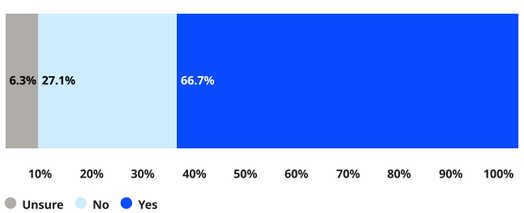


Base size = 55

Do you have internal expertise in cryptocurrency, blockchain or digital assets?

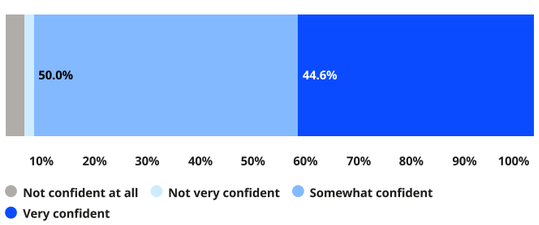
Base size = 56

Does use of cryptocurrency affect the level of risk assigned to a matter on file opening?



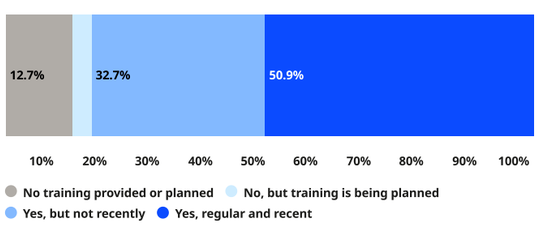
Base size = 48

How confident are you that your AML/CTF/KYC procedures adequately address the risks of clients using cryptocurrency as payment?



Base size = 56

Have your staff received any training on cryptocurrency-related risks (e.g., fraud, money laundering, tech risks)?



Base size = 55

In which areas of your firm's operations is Generative AI being used? Please select all that apply.

Legal research and analysis	74.7%
Document review	57.0%
Contract drafting and review	54.4%
Document automation and assembly	50.6%
Business development function	46.8%
Marketing function	46.8%
Compliance	45.6%
Due diligence	34.2%
Intellectual property analysis and management	30.4%
Customer relationship management (CRM) systems	30.4%
Calculation of claims	20.3%
Other	2.5%

Base size = 79

What steps has your firm implemented to address the risks associated with Generative AI and LLMs? Please select all that apply.

Internal policies and guidelines for the responsible use of Generative AI	75.0%
Providing training and education to employees on the risks and ethical considerations of Generative AI	68.3%
Monitoring legal and regulatory developments related to Generative AI	62.5%
Conducting risk assessments specific to Generative AI technologies	57.7%
Technical safeguards to prevent misuse or unauthorised access	57.7%
Prohibiting the use of Public Open-Source Generative AI (e.g. ChatGPT)	45.2%
Collaborating with external experts or organisations to stay informed on emerging risks	41.3%

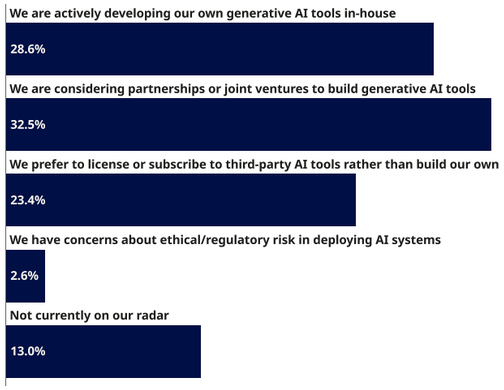
Base size = 104

What benefits has your firm experienced from using Generative AI technologies? Please select all that apply.

Increased efficiency and productivity	71.8%
Improved accuracy and quality of work	59.0%
Enhanced internal knowledge management or information retrieval	51.3%
Streamlined repetitive tasks	47.4%
Cost savings	44.9%
Enhanced client service and satisfaction	44.9%
Increased capacity to focus on higher-value legal work	41.0%
Boost innovation reputation or market positioning	30.8%
More scalable client service delivery	25.6%
Greater collaboration between legal, tech, and knowledge teams	21.8%
None	1.3%
Don't know	1.3%

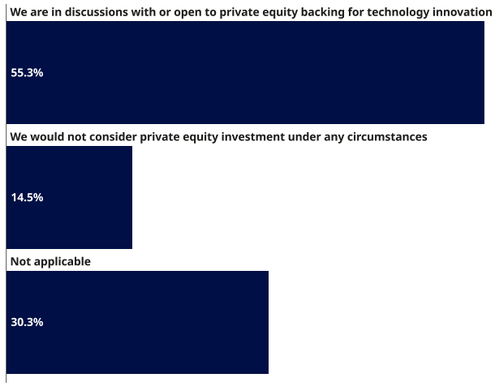
Base size = 78

To what extent is your firm exploring or engaging in the development of proprietary generative AI tools?



Base size = 77

Would private equity investment be considered as a route to fund AI innovation?



Base size = 76

In your view, what might unlawful or inappropriate use of Generative AI look like in a legal context? Please select all that apply.

Using AI-generated content without oversight or validation by a qualified lawyer	81.8%
Uploading client data into public or unvetted AI tools	68.8%
Generating misleading or deceptive content (e.g. deepfakes, false summaries)	68.8%
Submitting AI-generated content to courts or regulators without disclosure	55.8%
"Deep seek" use of AI to probe sensitive internal data beyond its intended scope	53.2%
Automating legal advice or decision-making without regulatory approval	50.6%
Bypassing ethical review or data governance processes when deploying AI tools	50.6%
Lack of transparency about AI use in client-facing services	45.5%
Using AI to monitor staff communications or productivity	36.4%
Other	1.3%

Base size = 77

Has the development of AI impacted the core requirements for hiring new lawyers in your firm?

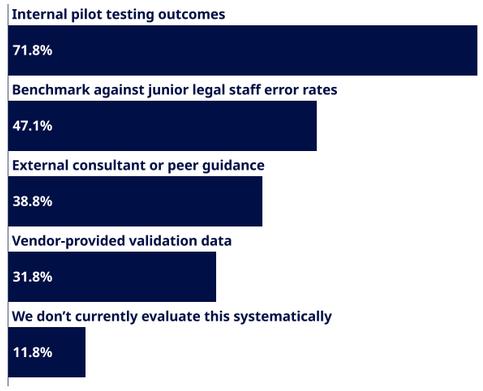
Base size = 77

What steps has your firm implemented to address the risks associated with Generative AI? Please select all that apply.

Internal policies and guidelines for the responsible use of Generative AI	81.8%
Providing training and education to employees on the risks and ethical considerations of Generative AI	72.7%
Monitoring legal and regulatory developments related to Generative AI	71.6%
Conducting risk assessments specific to Generative AI technologies	53.4%
Prohibiting the use of Public Open-Source Generative AI e.g. ChatGPT	43.2%
Technical safeguards to prevent misuse or unauthorised access	54.5%
Collaborating with external experts or organisations to stay informed on emerging risks	40.9%
Don't know	1.1%

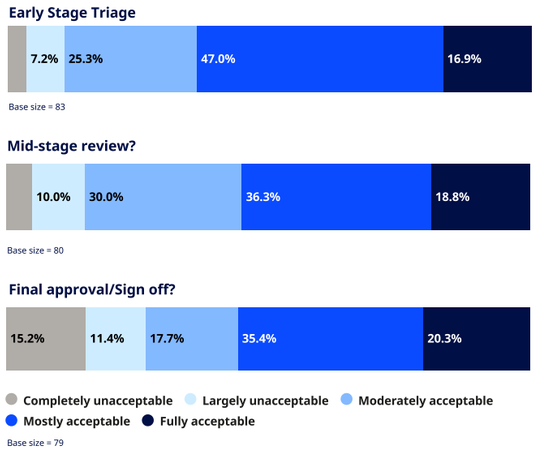
Base size = 88

How do you currently evaluate the reliability of AI tools in your workflow? Please select all that apply.

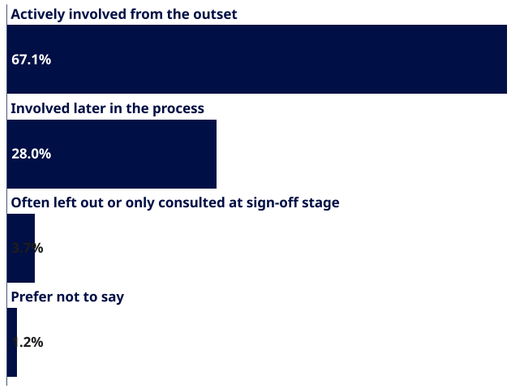


Base size = 85

How acceptable is the current AI error rate for your organisation's risk threshold at each of the following stages?



At what stage is the risk team generally involved in transformation conversations around internal legal technology and process at your firm?



In light of AI capabilities, what process redesign stage are you in?