Baker McKenzie.



2026

What's on the Radar for Financial Institutions?

Contents

03 **Fintech**

Agentic AI | M&A in fintech

07 **Corporate Responsibility**

Corporate fraud prevention | Sustainable Asian data centers | Workforce strategies

12 **Regulatory risk**

Cybersecurity | Deregulation | Digital currencies

16 **Global banks**

Sanctions | Tax | Wealth management

21 **Investment funds**

Private capital in Europe | Tokenization

25 **Regional Spotlight**

Islamic finance in the Middle East

Fintech



"The autonomous functionality at the heart of agentic AI holds out the prospect of exciting new use cases, such as payments, operating, for example, within digital platforms."

Vin Bange
Partner, London

Agentic AI

It's been a little more than three years since generative AI captured the public imagination, making a huge societal and business impact. Despite the excitement and promise held out by the technology, its impact on financial services has been less tangible than might have been expected. While it offers productivity and efficiency gains, many businesses in the financial sector are struggling to scale up generative AI effectively or balance perceived risk. The use cases that predominate today concern mostly transaction monitoring, summarizing research and due diligence, as well as writing technical documents, although many others remain under development. The emergence of agentic AI marks a turning point offering more tangible benefits to businesses and, importantly, to the financial sector. It marks a new stage in the development and adoption of AI.

Agentic AI refers to systems composed of groups of independent collaborative AI agents that can autonomously plan, execute and adapt complex tasks across multiple steps and domains against defined objectives. It can also use tools (e.g., web search, systems and other models and agents). Unlike generative AI, which needs specific prompts, humans should only be required for exception handling, oversight and coaching. Therefore, agentic AI takes us closer to the goal of artificial general intelligence; that is, it can understand, learn and apply knowledge across a wide range of tasks equivalent to a human being.

According to the MIT Technology Review (2025),

70%

of banking leaders report active or pilot deployments of agentic AI. Financial institutions will benefit from quicker processes, competitive advantages and cost-savings.

AI use already poses risks and challenges, including fairness (e.g., data bias), respect for intellectual property rights and the need to provide for contestability and redress. Agentic AI, with its autonomous nature, raises the stakes further. This derives in part from the design of governance and control frameworks that are hub-and-spoke in structure. The hub imposes a common control framework setting risk appetite, compliance and reporting standards. The spokes include compliance, risk management, AML/CTF, data privacy and security. Today, even with the advent of generative AI, there is a human at the center — monitoring and controlling the processes. In contrast, agentic AI takes the human out of the loop, as the autonomous nature of the technology means that it, rather than a human overseer, decides on which resources and processes are required for any specific task. Besides the legal question of who is responsible for outcomes, today's governance and control frameworks will likely be inadequate. They would require adaptation (or redesign) to properly assess the risks, to mitigate them and, of course, as inevitably will be the case, to prepare for occasional failures. In terms of business continuity, where AI processes fail, management in financial institutions should make provision, where practical, to fall back to manual processes.

Cybersecurity remains at the forefront of organizational concerns and is perceived as an especially high area of risk in the financial sector. AI is a double-edged sword; it can help boost cyber resilience while simultaneously increasing the potency of attacks, for example, by exploiting vulnerabilities faster than human attackers might do. Agentic AI raises the stakes. A successful cyberattack could exploit the central place that agentic AI occupies in a business's operations and processes, especially in the context where governance and control frameworks have not kept up with technological advances. Another aspect of the elevated cyber risk arising from agentic AI concerns financial institutions' own M&A where they merge or acquire other businesses to gain market share, innovative technology or new services. AI due diligence of the target is vital as it may be riddled with malevolent agentic AI capable of autonomous action. There is an increasing likelihood that this software may lie silent for months becoming operative only during the active phase of an M&A or initial public offering. In 2026 and in the future, these scenarios could become significant triggers for post-M&A disputes in the courts. Given the potential losses and regulatory penalties arising from the acquired business, suitable warranties and indemnities are essential.

The autonomous functionality at the heart of agentic AI holds out the prospect of exciting new use cases. Payments are also a hotbed for agentic AI opportunities, operating, for example, within digital platforms. The prospect of ordering a new outfit for a wedding next weekend just by setting parameters and letting agentic AI do the rest, including making the payment, is enticing for many consumers. However, the legal framework and payment scheme rules will need to adapt to keep up, which is something to watch for 2026. In the field of personalized financial planning, AI agents could act as virtual advisers, tailoring investment, tax and retirement strategies, by engaging with clients across multiple communication channels adapting to client preferences.

In this context, it's possible, for example, that personal data could be used or repurposed by this technology in ways never envisaged. Here lie significant legal and regulatory risks for financial institutions (like other businesses) arising from legal requirements governing data privacy, transparency and fairness. Those jurisdictions that afford more flexibility are likely to benefit from more investment, allowing businesses the opportunity to better test and develop the potential of AI. The UK, for instance, is taking advantage of its ability to diverge post-Brexit from the EU GDPR, having amended its legislation, with the Information Commissioner's Office expected to update its guidance on the purpose limitation principle to provide for greater flexibility. Those jurisdictions that adopt a flexible, principles-based regulatory architecture for AI are likely to see more investment in and development of this technology. This is especially relevant to agentic AI, which, due to its autonomous and wider reaching nature, may more readily find friction with detailed rules-based regulation. It's also important that financial regulators support its development and facilitate, for example, regulatory sandboxes for testing agentic AI in controlled environments.

M&A in fintech

The momentum of M&A in fintech returned in 2025, with fewer deals but bigger valuations. The trend leading into 2026 sees many dealmakers focusing on where strategic logic is strongest and financing is available. Of these, financial services remain among the most active verticals by value, with payments once again leading in consolidation figures. As we look ahead to 2026, M&A activity in this sector is set for a promising year, shaped by accelerating regulatory recalibration and stabilization, strategic repositioning by financial institutions and the ever-increasing influence of AI in investment decision-making.



> "2026 is likely to be a year of strategic, tech-driven M&A, seeing continued consolidation in key verticals and increasingly AI-influenced investments, with participants navigating regulation cautiously, looking to enhance their competitiveness in a steadily digitalizing economy."

Ashlin Perumall
Partner, Johannesburg

Fintech firms and platforms remain attractive targets for financial institutions, particularly those offering scalable solutions in payments, compliance automation (i.e., fraud prevention) and embedded finance. As legacy systems become increasingly unsustainable, incumbents in both the banking and nonbanking financial sectors are seeking bolt-on acquisitions to speed up their digital transformation. Outside of the big-ticket deals, mid-market roll-ups and corridor coverage deals are also likely to continue to feature in 2026. This includes cross-border FX and account-to-account payment players, which can stitch together diverse licensing regimes, such as the Baltics, UK/EU and Africa, to widen payout corridors and enable regulatory passporting. Stablecoin rails for such corridor coverage is increasing interest in deals in this sector, with many jurisdictions emboldened in investment since the US GENIUS Act.

AI is now a growing force reshaping the landscape. Banks are beginning to transition from pilot projects and chatbots to embedded AI, driving demand for better data plumbing solutions, the development of orchestration frameworks (i.e., systems that manage and coordinate the interaction of software components, services or agents, and AI talent) and safety controls. AI is already beginning to mature in credit-scoring and AML/CTF compliance, but it is still emergent in agentic AI — autonomous systems capable of reasoning and executing complex workflows — where ROI is uneven and nascent. Nonetheless, the high levels of return predicted by fintechs on AI investments exemplify the strategic value underpinning such deals — nearly half of all venture capital funding now goes to AI-centric firms — signaling a growing appetite for innovation-led growth.

Fintech also remains a priority sector for private equity and venture capital investment. This trend is expected to fuel consolidation among mid-sized tech players, especially those struggling to scale independently. There is, for example, intensifying competition in both the asset and wealth management sectors, where technological change is bringing new impetus to drive M&A activity as financial institutions seek to consolidate and achieve efficiencies.

Regulatory scrutiny will remain a key consideration. The fintech sector, in developing new technologies, often operates in an environment where regulation is either out of date or nonexistent. This creates varying levels of uncertainty for many business models. The reality of changing laws and transactions is frequently an unhelpful material factor in M&A deals. For example, until recently, uncertainty over the regulatory status of crypto assets in the US was a major obstacle to the asset class's growth in the world's largest economy. By 2026, greater clarity on crypto is expected with the GENIUS Act in the US and the implementation of similar laws in other jurisdictions. Similarly, other regulatory milestones are anticipated in 2026. For instance, Markets in Crypto-Assets Regulation transitions will extend toward mid-2026, meaning crypto-asset service provider-portability and license passporting will be relevant in EU transactions. Additionally, the Digital Operational Resilience Act will have a greater impact in 2026, shifting the focus for fintech firms from initial planning to demonstrating operational compliance in practice, as supervisory activities and audits increase and become more important in due diligence and warranties during M&A processes. Furthermore, from August 2026, the EU AI Act will subject high-risk AI systems, such as credit scoring and insurance risk assessment firms, to regulatory oversight, and buyers will likely value fintech targets in these sectors based on assessment roadmaps.

In sum, 2026 is likely to be a year of strategic, tech-driven M&A, incorporating both continued consolidation in key verticals and increasing AI-influenced investments with participants navigating regulation cautiously, looking to enhance their competitiveness in an increasingly digital economy.

Corporate Responsibility



"Senior managers need to show how they have met their obligations, as laws and law enforcement increasingly hold them and their employers to account."

Henry Garfield
Partner, London

Corporate fraud prevention

Internationally, there is a growing focus on the prevention of financial crime and accountability in the corporate world. Financial institutions are no exception. In particular, individuals and their employers are more likely than ever to face prosecution or enforcement action for facilitating misconduct by others. In the most egregious cases, penalties and settlements have run into hundreds of millions of dollars and prison sentences have been significant.

In the UK, specific offenses relating to bribery, taxation and, more recently, fraud, make it easier to prosecute businesses by introducing corporate criminal liability for failing to prevent such wrongdoing by associated persons, including employees. To be prosecuted for these offenses, the company need not know about the underlying criminal conduct committed by those associated with it: they are criminally liable for failing to prevent it. The new fraud offense (in force since September 2025) covers conduct such as employees engaging in dishonest sales practices, hiding important information from investors or borrowers, or engaging in dishonest practices in financial markets (providing they benefit their employer). Even foreign financial institutions can be liable where the underlying fraud offense has a UK ~nexus, for example, accepting deposits from UK customers, even without a UK branch or subsidiary. Put very broadly, if a person associated with the company (including employees) commits one of these specified fraud offenses for the benefit of the company, the company can be prosecuted for failing to prevent fraud. The only defense is that the company had in place reasonable procedures to prevent the fraud in the first place.

Alongside the new failure to prevent fraud law, the law in the UK on corporate attribution has also changed. Previously, to prosecute a company for most financial crime offenses, prosecutors had to show that those acting for a business were its "directing mind and will" — a very high burden.

This burden was, in practice, even higher for large financial institutions where significant decisions are regularly taken by individuals and committees outside the main board. Now, attribution will extend to the acts of "senior managers," which will likely include senior executives below board level. Together, these changes significantly lower the barriers for prosecutors to bring corporate prosecutions in the UK. At the same time, the Financial Conduct Authority (FCA) and UK prosecutors are more focused than ever on individual wrongdoers and bringing them swiftly to account. The Serious Fraud Office (SFO) has also recently updated its corporate cooperation guidance, signaling that it will reward self-reporting, cooperation and prompt remediation. Similar considerations are relevant for FCA action.

The US Sarbanes-Oxley Act of 2002 was passed in response to a series of notorious financial frauds. It strengthened financial reporting and internal control requirements for public companies. Managers must annually assess and document internal controls over financial reporting, attested by an independent auditor for larger corporates. We now see external auditors apply higher standards, such as

comprehensive risk assessments and documentation of automated IT systems, including systems driven by AI. This is especially relevant for rapidly growing fintechs that may experience gaps in their controls. Compliance now includes environmental, social and governance data, where greenwashing risk should be high on management's priorities. Under its recent White-Collar Enforcement Plan, the Department of Justice is targeting fraud against investors and markets, including investment fraud and complex money laundering.

The SEC's Enforcement Division, under new leadership, has renewed its focus on insider dealing, market manipulation and accounting fraud. It emphasizes holding executives personally liable for wrongdoing instead of imposing fines on entities as a cost of doing business.

Rather than enforce technical rule breaches, the SEC will investigate misconduct that impacts retail investors and damages confidence in the market. However, recent SEC enforcement actions have involved settlements with investment advisers and fund managers on non-fraud related violations, such as violations of marketing and custody rules. This may signal a particular focus on conduct of fiduciaries. As with the SFO, the SEC has also signaled that it will reward self-reporting, cooperation and prompt remediation. Credible internal investigation of potential misconduct should remain a priority.

Elsewhere, reflecting these trends, the Australian Securities and Investments Commission (ASIC) is sharpening its enforcement focus on personal liability for governance failures. Its 2025-2026 Corporate Plan and enforcement priorities highlight systemic compliance failures, misleading conduct and breaches of directors' duties as enduring concerns. Looking ahead, ASIC is expected to intensify scrutiny of board-level accountability, especially in superannuation and investment governance. The Australian Prudential Regulation Authority's parallel warnings to superannuation trustees — "you cannot outsource accountability" — signal a coordinated regulatory stance as ASIC increasingly targets individuals for enforcement, not just entities.

Despite several high-profile cases, because financial institutions are already highly regulated (i.e., applying strict systems and controls and senior management responsibilities), they should be well placed in terms of policies and procedures, as well as culture, to deal with the changes identified above. However, leadership should review their adequacy, resourcing and currency for 2026, especially given technological developments, the compliance environment, evolving law and regulation and the changing geopolitical environment. Risk assessments should be brushed off and refreshed. Board oversight should be strengthened to ensure accurate disclosures and good audit trails. Senior managers need to show how they have met their obligations in a context where law and enforcement will more readily hold them and their employers to account.

Sustainable Asian data centers

Data centers and associated infrastructure are a dynamic and fast-moving sector in Southeast Asia (as elsewhere) driven by the growth of the region's digital economy. While financial return is determinative, sustainability (less the recent hype) remains an important consideration for those developing, operating and financing data centers. This reflects investor and end user expectations and increasing scrutiny over the resources they consume. There are issues around land use and "embodied" carbon from building materials necessitating strategies to minimize the impact. Operating these assets also raises sustainability concerns, as AI workloads are especially energy intensive with significant power and cooling requirements leading to rising emissions.

To illustrate, data centers currently use

1.5% to 3%

of global electricity, with projections suggesting this could double by 2030 (IEA, Energy and AI, April 2025).

Across Asia Pacific, it is estimated that only

32%

of demand will be met by renewable energy (PwC).

With rapidly growing demand for more capacity, there is a risk that sustainability considerations may be deprioritized. Given developing sustainability standards, this may be counterintuitive. In any event, the efficient use of resources is not incompatible with bringing new data centers into operation expeditiously and efficiently. Currently, there are no specific global standards on what represents a sustainable data center, making comparisons difficult. However, with the degree of focus now on the sector, this is likely to change in the future. Pointing the way in 2025, the United Nations Environment Programme published new procurement guidelines for data centers and servers. As an example, Singapore, Malaysia, Indonesia and other countries in the region are actively promoting sustainability. In 2024, Singapore published a Green Data Centre Roadmap for a sustainable pathway for their continued growth, through best-in-class energy efficiency and the use of green energy. Malaysia's Digital Economy Blueprint aspires for Malaysia to be "a regional leader in the digital economy and to achieve inclusive, responsible and sustainable socioeconomic development ."

Sustainable finance is an important funding opportunity and tool to enable developers and operators to align finance with key performance indicators, for example, on carbon, energy and water usage, which will often also align with end user targets. It is also important to mitigate potential liabilities for environmental and sustainability risks given the extensive use of natural resources. This can be done through requiring compliance with market-standard formal green principles, e.g., the Green Loan Principles issued by the Asia Pacific Loan Market Association and corresponding representations and covenants. By linking the borrowing cost of a project to the operator's sustainability performance, this incentivizes energy efficiency and carbon footprint reduction. A formalized commitment to climate goals and energy efficiency enhances an operator's reputation in the market and can make a project more attractive to investors and end users.

The sector should prioritize embedding sustainability and resilience requirements at a time when so much investment is being made, to align with investor and customer requirements and to avoid remediation steps at a later stage.



"Data centers should prioritize embedding sustainability and resilience requirements at a time when so much investment is being made, to align with investor and customer requirements and to avoid remediation steps at a later stage.

Aaron Jones
Local Principal, Singapore

Workforce strategies

As financial institutions recalibrate their workforce strategies for 2026 and beyond, they face a rapidly shifting regulatory terrain shaped by geopolitical tensions, technological disruption and evolving societal expectations. 2025 has seen a marked acceleration in legal reforms and policy shifts across jurisdictions, with five key themes emerging at the forefront of employment and compliance planning. These trends are not isolated — they are interconnected, and they demand a proactive, globally attuned approach to workforce governance.

While institutional diversity, equity and inclusion (DEI) programs and practices have been subject to more legal scrutiny in the US this year, other regions—particularly EMEA and parts of Asia—are deepening commitments and expanding regulatory requirements. Major US-based financial institutions have scaled back public commitments to DEI, rebranding or removing references to diversity figures and programs in corporate filings, amid heightened political scrutiny under the current US administration. In contrast, many financial institutions across EMEA remain committed to robust DEI frameworks. For example, the UK's financial regulators have proposed regulatory standards to embed diversity and inclusion into governance structures. And in South Africa, financial and insurance activities is a sector specifically identified under new affirmative action targets now in force. This divergence underscores the need for multinational financial institutions to carefully navigate DEI policy and goals with regional nuance, balancing local regulatory pressures with global values and workforce expectations.

Employers, including those in the financial sector, are under pressure (from both employees and government authorities) to increase transparency, particularly on workforce composition and compensation. In Brazil, for example, equal pay enforcement has intensified, with hundreds of companies inspected in the last year. Some of the significant changes include the US, where certain states, including California, require gender pay reporting, and shareholder activism is driving pay equity disclosures. In the EU, the Pay Transparency Directive requires member states to implement legislation by June 2026, with gender pay gap reporting starting in June 2027. Key requirements include: mandatory pay range disclosure; banning salary history questions; and employee rights to pay information with an increased role overall for worker representatives.

AI adoption in HR functions is surging, but so is regulatory oversight. The EU's AI Act, for example, mandates transparency, risk-based controls and involvement of worker representatives. A number of jurisdictions in North and Latin America have introduced or are reviewing AI bills with employment-related provisions. In the US, state and other local laws impose strict notice and consent requirements relating to certain automated decision-making technology. Japan has adopted a voluntary, soft-law approach, issuing ethical guidelines focused on transparency and societal impact to influence corporate behavior in areas like recruitment and employee monitoring, while governments in both Australia and Singapore are introducing sandbox environments and governance frameworks for responsible AI use. Employers must now map AI-related risks across jurisdictions, implement governance protocols and prepare for audits and whistleblower protections.

Jurisdictions are imposing proactive obligations on employers to prevent workplace harassment. New laws mandate employer action against harassment and workplace violence in Chile and Colombia; meanwhile, Asia Pacific jurisdictions including Australia, Japan, China and Taiwan require employers to proactively prevent sexual harassment, with new compliance frameworks emerging.



"While DEI programs and practices have been subject to more legal scrutiny in the US this year, other regions—particularly EMEA and parts of Asia— are deepening commitments and expanding regulatory requirements."

Kim Franko
Partner, New York

In the UK, a new legal duty will require employers to take all reasonable steps (including third-party misconduct) to prevent sexual harassment, while in the Netherlands, employers with 10 or more employees will soon need to have a code of conduct to prevent improper conduct in the workplace.

While demand for top talent remains high, financial institutions continue to focus on business protection risks that arise when employees leave the organization. They are looking to enforceability of post-termination restrictions and traditional confidentiality obligations, while strengthening employee exit procedures. Financial institutions in Hong Kong, Singapore, Japan and Korea are recalibrating hiring strategies to respond to renewed deal activity, leading to more frequent cross-border moves and lateral hiring across jurisdictions. This heightened mobility has placed greater emphasis on cross-border enforcement of restrictive covenants and confidentiality obligations. As a result, firms are adopting more sophisticated approaches to protecting business assets at the point of termination. These include tailored exit protocols, forensic audits of departing employees' digital footprints and the use of garden leave (where legally permitted) to mitigate competitive risk. There is also growing global interest in contractual mechanisms, such as clawbacks and deferred compensation structures, to discourage premature departures and protect proprietary information.

Regulatory risk



"It's essential that contractual frameworks set industry best standards for cybersecurity and hygiene, including reporting obligations and audit rights, and have clear risk allocation and indemnity language."

Christoph Kurth
Partner, Zurich

Cybersecurity

Financial services is one of the most targeted sectors in the economy. According to CrowdStrike, cyberattacks are escalating in speed, volume and sophistication.

Two thirds

of financial institutions worldwide reported ransomware attacks in 2025, a sharp rise from 34% in 2021 (Statista).

A notable feature of the threat landscape is the human element. Instead of relying on sophisticated malware, cyber delinquents are increasingly exploiting social engineering vis-à-vis employees to bypass security and access IT systems, to be precise, through vishing (i.e., voice phishing) where cybercriminals phone individuals to trick them into performing actions that compromise security. Low cost and readily available generative AI can facilitate deception, for example, with false texts and fake profile images or by cloning a manager's voice. This is where staff training and an awareness of cyber threats and common subterfuges are so important. Training forms an integral part of operational resilience and regulators expect it to be in place. The temptation to roll out tick box programs must be avoided, ensuring training is repeated, tailored to staff roles and consistent with risk assessments. The importance of everyone's behavior should be reinforced by senior management.

Cyber-specific regulations apply to ever more organizations, not only critical infrastructure providers, but a broader range of digital service providers and businesses offering products with digital elements. The EU's Digital Operational Resilience Act and NIS 2 legislation are examples. Regulations related to the digital space or cyberspace often have extraterritorial effect. Organizations must document and implement proportionate risk measures — via an information security and management system — in accordance with prevalent industry standards, where management is held accountable for failures.

Cyber resilience and responsibilities extend beyond a business's own systems. Today, risk from outsourcers is equally important. Who do you depend on for critical services, which, if disrupted, would impact your operations or might facilitate a cyberattack? Cloud service providers and their data depositaries are one such vulnerability. For this reason, third- and (even) fourth-party due diligence is essential. Are their capabilities equivalent to yours and are you collaborating with them? It's essential that contractual frameworks set industry best standards for cybersecurity and hygiene, including reporting obligations and audit rights, and that they have clear risk allocation and indemnity language.

While it's getting tougher to protect your business, incident reporting and notifications obligations are also a growing burden. Data protection and privacy legislation has been in place for some time, but there is a developing framework of financial regulatory obligations such as the US SEC Cyber Disclosure Rule

for publicly traded companies. The timescales and the detail can be challenging — especially when managers' attention is on resolving an attack. For financial institutions that have a presence in multiple jurisdictions this calls for significant resources, input from legal and compliance, and executive oversight.

Deregulation

Financial services were at a crossroads in 2025, shaped by a wave of deregulation initiated by the new US administration and mirrored, to varying degrees, in other major economies. This is driven by a desire to shake up the existing order, boost sluggish economic growth and address perceived overreactions to the 2008 global financial crisis. As regulators and participants recalibrate, the sector faces both opportunities and risks, with implications for market participants, investors and legal counsel worldwide.

The US has embarked on an aggressive deregulatory agenda. President Trump has issued executive orders intended to address overregulation, such as the "10-for-1 Rule," requiring agencies to identify

10

existing regulations for repeal for every new regulation introduced.

The White House has increased its oversight of executive agencies, signaling a new era of centralized regulatory control.

The SEC has initiated its own deregulatory agenda. Notably, it has pivoted away from regulating through enforcement actions, focusing on protecting investors from fraud and Ponzi schemes. This has led to reduced headcounts within the SEC's enforcement division. Additionally, it has eased regulatory burdens on issuers and is encouraging the growth of retail investors in private markets. Bespoke ESG rules are no longer being pursued by the SEC. The focus has shifted to simple, accurate and fulsome disclosure, echoing similar moves in the EU, where there are efforts to water down ESG legislation. US pressure has led to concessions for third-country companies from reporting and disclosure requirements, and in Asia Pacific, sustainability measures have taken a back seat to business-as-usual priorities.

Other regulators are reducing headcount — or are subject to restructuring or, in some cases, dismantlement. For example, although it is the subject of continued litigation, deep staff cuts are underway at the Consumer Financial Protection Bureau, originally created in 2008 to protect consumers. This signals a shift back to pre-2008 regulation.

Additionally, the Office of the Comptroller of the Currency recently cut

76

probationary staffers.

While the Public Company Accounting Oversight Board has survived, uncertainty abounds, as efforts to defund, reduce headcount and incorporate it into an office within the SEC continue.

Bank regulators have eased capital requirements, and there is potential for a reversal of executive orders restricting bank consolidation. The UK has followed the lead of the US in some respects, easing bank bonus and risk management rules. However, Switzerland has proposed increasing minimum capital requirements on systemically important banks, reflecting a more cautious regulatory stance.

The passage of the GENIUS Act, which establishes the regulatory framework for US stablecoins, and the potential passage of the CLARITY Act, brings a new era of digital asset regulation in the US, though much work remains as this legislation is implemented. Emerging technologies, especially AI and digital assets, are reshaping the regulatory landscape. Regulators are grappling with how to govern the use of AI and how to regulate digital assets. On AI, the tension between principles-based and prescriptive approaches will continue to define regulatory debates, with the US and the UK favoring flexibility and the EU and China opting for more rigid frameworks. In the early 2000s, the US largely dictated how the internet was regulated globally. It remains to be seen whether a single AI regulatory approach will prevail, or if a patchwork of approaches will emerge as countries assert greater regulatory control within their spheres of influence.

Easing regulatory burdens can drive growth and innovation. That the SEC will not test new regulation through specious enforcement actions should provide comfort to those acting in good faith. And those that can act swiftly in response to new tech regulation will gain first-mover advantage. Internationally, the divergence in regulatory approaches is creating opportunities for regulatory arbitrage, strategic repositioning and valuation gaps. The interconnectedness of financial markets means that changes in one jurisdiction can have effects globally, necessitating adaptability among market participants.

In 2026, the deregulation buzzword will continue to be "volatility." While deregulation will remain, expect it to be subject to litigation and a difficult legislative environment. In the US, current initiatives enjoying some bipartisan support could stall in the lead up to the 2026 midterm elections. However, deregulation does not mean no regulation. And for participants operating a global platform, taking advantage of deregulation in any one country on a cost-effective basis may be more difficult than it appears, especially as some US states ramp up efforts to take the place of federal regulators.



"The SEC has initiated its own deregulatory agenda. Notably, it has pivoted away from regulating through enforcement actions, focusing on protecting investors from fraud and Ponzi schemes."

James Linhardt
Counsel, Chicago

Digital currencies

2026 will be a key year for stablecoins and their counterparts, central bank digital currencies (CBDCs), which promise to disrupt the business models of traditional banks and payment providers. US dollar denominated stablecoin market capitalization has grown in less than two years from USD 125 billion to around USD 255 billion today (BIS).

It could grow to

USD 2 trillion

USD 2 trillion in the next few years. Bank supervisors are backing CBDCs in response to the threat posed to their monetary dominance.

Blockchain-driven digital currencies, with their use at scale, could force incumbents to revisit their business models based on existing payment rails and, critically, the holding of customers' deposits. In the case of CBDCs, (save for privacy concerns) many depositors may prefer to use central bank accounts, to avoid bank runs such as during the 2023 US regional banking crisis. Like CBDCs, stablecoins promise to make payments easier and, coupled with an electronic payments wallet, lessen the need for bank accounts and the current (often) slow and (relatively) expensive payments infrastructure.

In the US, the GENIUS Act introduces a regulatory regime for stablecoins that offers market integrity and consumer protection, renewing the impetus around their use in the world's largest economy. Elsewhere, for example, in the Hong Kong SAR, the Stablecoins Ordinance establishes a licensing regime for issuers and related activities with applications for licenses now open. In other jurisdictions such as the EU, UAE, India, Japan and Singapore, besides their own stablecoins, CBDC initiatives are in sight of becoming operational. India has piloted a digital rupee under the tagline "Cash, but Digital." In Africa, CBDC incentives include improving financial inclusion among the unbanked.

Some worry that stablecoins and CBDCs will cause an outflow of deposits from banks. According to the Bank for International Settlements, this is especially likely when stablecoins are backed by high-quality liquid assets and offer features similar to money market funds. So, banks face a risk of disintermediation, and with it a loss of fees for facilitating payments and access to cheap deposits for lending. Some jurisdictions propose to restrict retail or limit CBDCs to wholesale purposes.
In contrast to its supportive approach to stablecoins, the US may ban a retail CBDC, on the grounds of privacy, surveillance risk and government overreach. A further concern is the economic effect of diminishing the multiplier effect whereby banks, in effect, create credit by lending deposits out multiple times. Overall, though, a combination of limits on holdings and non-interest bearing accounts should reduce any impact.

Authorization and stringent conduct and prudential requirements will be needed to issue stablecoin, so banks will likely still have an advantage over newer nonbank entrants. However, competition is likely to grow, especially from tech companies benefitting from greater confidence over stablecoins and lower entry costs due to new technologies. They may also benefit from the ambiguity between a regulated financial service and an ancillary technical service (e.g., the software behind a payment wallet).

Global banks, where permitted, are exploring the issue of their own stablecoins pegged to the dollar (or to the euro), facilitating the movement of funds not only out of but back into deposits. Similarly, international payments entities are looking to modernize cross-border transactions using blockchain, including stablecoins and tokenized deposits to facilitate transactions. Banks should leverage customers' trust and guide them through evolving financial infrastructure, and in doing so promote their own digital products such as payments, custody and as stablecoin reserve holders.



"International payments entities are looking to modernize cross-border transactions using blockchain, including stablecoins and tokenized deposits to facilitate transactions."

Karen Man
Partner, Hong Kong

Global banks



"Third-party risks are a critical concern; financial institutions must ensure that they consider sanctions risk associated with all parties involved in a transaction, especially those with complex ownership structures."

Terry Gilroy
Partner, New York

Sanctions

Geopolitical uncertainty means sanctions can be imposed with little notice. Banks must quickly adjust their compliance and risk frameworks in response to geopolitical events such as Russia's invasion of Ukraine in 2022 and the change of regime in Syria in late 2024. Looking ahead, 2026 may see further US secondary sanctions on Chinese banks to curtail China's financial support for Russia's war in Ukraine. Financial institutions must ensure that geopolitical risk analysis is at the center of their considerations. Contingency planning is essential and good communication with regulatory bodies is crucial.

So, let's consider some of the challenges for the coming year. There's regulatory complexity. There are a multitude of sanctions lists and regulations from the EU, the UK and the US, each with its own nuances and requirements. There is a lack of harmonization across jurisdictions. For instance, while the EU's sanctions regime and that of the US Office of Foreign Assets Control (OFAC) may be similar and have the same goal with respect to certain programs (e.g., Russia), their precise scope and exceptions may differ. For example, in the EU, member states will each enforce and interpret EU measures differently and take varying approaches to granting licenses and waivers. Banks need to invest resources to achieve a holistic view of sanctions, their interrelationship and how they affect their activities and those of counterparties. Tracking changes in sanctions is essential.

Third-party risks are a critical concern; financial institutions must ensure that they consider sanctions risk associated with all parties involved in a transaction, in particular those with complex ownership structures.

Just considering designated persons, there are approximately

80,000

persons globally.

The importance of thorough due diligence and continuous monitoring cannot be overstated. Technologies, such as AI and machine learning, can provide real-time monitoring and identify potential red flags. By adopting a proactive and well-resourced approach, banks can better avoid the severe consequences of noncompliance.

Banks should expect more litigation from sanctions-related disputes with counterparties; as such, reviewing terms and conditions for contractual protection is critical. Common scenarios include where payments cannot be made, for example, by the trustee of a syndicated loan or a securities depository. Financial institutions, in particular, must be mindful of reporting obligations that will differ across jurisdictions. They should maintain a dialogue with regulators and, where permitted, explain the position with clients and counterparties, and use best endeavors to comply with contractual obligations.

This year will see a continued ramping up of sanctions enforcement. The US has widened the application of secondary sanctions against non-US financial institutions that engage in "significant" transactions with designated persons. OFAC is also enforcing against individuals who try to obfuscate and conceal sanctions evasion within businesses. Export control compliance is a growing issue for financial institutions, with the US Commerce Department partnering with the US Financial Crimes Enforcement Network to encourage more reporting on financial transactions that implicate US export controls. Similarly in Europe, enforcement is intensifying. The UK applies strict liability and has strengthened its Office of Financial Sanctions Implementation enforcement capabilities.

Tax

Global bank leadership can expect further change in the international tax landscape in 2026. Areas of focus are likely to include the first reporting under the OECD's Pillar Two framework, the updated Common Reporting Standard, an increased focus on the tax implications of greater global mobility, the evolving nature of VAT exemptions for financial services and further integration of tax and sustainability. Preparedness is key as banks will need to stay abreast of, and respond to these developments.

Around half of the

140

jurisdictions that signed up to the Pillar Two framework for a global minimum tax have enacted legislation and are gearing up for the first returns to be filed from June 2026.

Global banks will need to ensure that systems are set up to collect the data required to undertake the complex Pillar Two calculations and to meet new compliance obligations.

To add to this, on 5 January the OECD Inclusive Framework reached agreement on the long-awaited "side-by-side" system with the US (agreed in principle by the G7 in June 2025 to exempt US-parented groups from certain Pillar Two taxes) and announced several safe harbors intended to streamline compliance obligations for applicable groups going forwards. These changes will now need to be implemented into domestic law by jurisdictions, whilst further work continues at OECD level on other aspects of the regime. Banks should actively monitor and prepare for evolving Pillar Two requirements in 2026.

Banks should also be aware that the updated Common Reporting Standard — CRS 2.0 — comes into effect in many jurisdictions in January 2026, and they should ensure due diligence procedures and data collection systems are ready for 2026 reporting.

The rise of remote work and internationally mobile employees has increased tax uncertainty for businesses, exposing them to risks around employment taxes, social security, corporate tax residency and permanent establishment issues. The OECD has recently issued new guidance on how cross-border "home office" arrangements are treated for permanent establishment purposes, which is intended to provide greater certainty in this area.

The indirect tax landscape brings a series of new challenges due to the complex and ever-evolving nature of VAT exemptions for financial services given increasing litigation and changing administrative practices. Global banks face scrutiny on their intercompany outsourcing arrangements coupled with an increasing tension between VAT and transfer pricing rules. Furthermore, banks must navigate diverging global regulations and the digitization of tax systems, including new e-invoicing and real-time reporting mandates. Successfully managing this complexity demands significant investment, particularly as indirect tax represents a substantial cost for businesses.

The global sustainability framework continues to mature, with the proliferation of sustainability regulations and market-driven pressures, despite geopolitical headwinds. In that context, tax is increasingly recognized as an important tool, with the conversation evolving from "whether" to "how" businesses can integrate tax and sustainability.

With tax transparency becoming established as the default, organizations are increasingly engaging in discussions about the material impact of tax in sustainability disclosures. These discussions require careful assessment to manage stakeholder expectations, complete financial and sustainability narratives and manage legal risks. The prominence of tax factors in ESG ratings and the change in risk-perception parameters around tax responsibility are growing, with clear evidence that tax responsibility is now part of a broader assessment of business strategies and long-term resilience.

Finally, climate-related tax measures pricing externalities are likely to become a permanent cost in balance sheets but should also be seen as triggers for innovation. In short, the integration of tax and sustainability has the potential to foster business resilience and trust with a growing pool of stakeholders.



"Preparedness is key as banks will need to stay abreast of, and respond to, critical tax, regulatory and other legal developments as the international tax and regulatory landscape evolves."

Natalie Dunne
Partner, London

Wealth management

The global wealth management industry is undergoing profound transformation, driven by regulatory shifts, geopolitical tensions and technological disruption. Banks, as central players in this ecosystem, face mounting challenges in maintaining compliance, managing risk and sustaining client trust.

In the US, the reelection of President Trump has ushered in a deregulatory wave. While this promises reduced compliance costs and greater operational flexibility, it also introduces uncertainty. Financial institutions must now navigate a fragmented regulatory environment, balancing relaxed fiduciary standards with heightened scrutiny in areas like cybersecurity, environmental, social and governance disclosures, and AI governance. Litigation risks are also rising. The average legal settlements in the wealth sector are said to be higher than in the past in the US, with reputational damage and increased debt-to-equity ratios impacting firms' capital valuations. Regulatory enforcement remains active, particularly around marketing practices and electronic communications, with the SEC imposing multimillion-dollar fines for noncompliance.

Banks are contending with a complex risk matrix. According to the US Office of the Comptroller of the Currency, top concerns include credit risk from commercial real estate, cyber threats and compliance pressures from evolving AI and AML regulations. The adoption of AI, while promising operational efficiency, also raises concerns about transparency, bias and regulatory oversight. Moreover, geopolitical instability and economic volatility have increased refinancing risks and market unpredictability, prompting banks to reassess their risk management frameworks.

Private banks must now ensure robust KYC procedures, source-of-wealth verification and transaction monitoring. Failure to comply can result in severe penalties, reputational damage and even criminal liability. The legal burden is compounded by the proliferation of digital assets and fintech platforms, which require new risk controls and regulatory interpretations.

Switzerland remains a global leader in cross-border wealth management, managing over

CHF 3.1 trillion

in assets.

However, its private banking sector, once synonymous with discretion and stability, is undergoing a regulatory transformation. The Swiss Financial Market Supervisory Authority (FINMA) has significantly tightened AML provisions, emphasizing conduct and transaction analysis over mere documentation.

Banks are now required to corroborate client wealth sources and monitor for inconsistencies, making compliance more resource-intensive but also more effective. Recent enforcement actions underscore the shift. Swiss authorities have levied multimillion-franc fines against larger Swiss private banks for AML breaches and misconduct in international scandals. These cases highlight the reputational and financial risks of inadequate legal oversight.

Further, FINMA and the Swiss National Bank have emphasized the importance of capital adequacy, liquidity and stress testing, particularly for domestically focused systemically important banks. Regulatory burdens around ESG, digital assets and transparency are increasing operational complexity but also driving innovation. Finally, Switzerland will tighten its regulatory regime following the collapse of Credit Suisse. In particular, there are heated political discussions about imposing stricter capital requirements on systemically important banks.



"To thrive in wealth management's evolving landscape, banks and wealth managers must embrace technology, invest in compliance infrastructure and develop agile strategies."

Dr. Ansgar Schott
Partner, Zurich

To thrive in this evolving landscape, banks and wealth managers must embrace technology, invest in compliance infrastructure and develop agile strategies. Leveraging AI for regulatory reporting and client profiling is becoming a competitive differentiator. Ultimately, those that succeed will have transformed legal and regulatory challenges into opportunities for innovation, trust-building and sustainable growth.

Investment funds



"European authorities are scrutinizing private capital to boost transparency, including the use of stress testing. This opens the possibility of heightened regulation and more disclosure."

Carlo de Vito Piscicelli
Partner, Milan

Private capital in Europe

Compared to the US, the growth of private capital trails behind in Europe, but this is changing. Given a more difficult market in the US, private capital is looking toward the region. Private equity, which has been quiet recently, is experiencing a resurgence of deal activity, while in private credit, direct lending has become a real alternative to traditional banks with many private debt products now available. A key dynamic is the data center boom (driven by generative AI) needing significant sums to finance construction. As evidence of changing European attitudes, Germany, long hostile to private equity, is seeing its banks fundraising from wealthier clients and, incidentally, in so doing, challenging the preeminent position of institutional investors. However, with anemic GDP growth, market confidence remains fragile.

2026 is a year to watch for regulatory developments — some beneficial, others less so. Given high debt levels and increasing credit delinquency, especially in the US, supervisors are concerned about systemic risk. Lightly regulated private capital and financial institutions are increasingly interconnected and their lending to each other is opaque. Debt structures are ever more complex. The IMF recognizes that partnerships between private credit, banks and insurers bring significant economic benefits. However, it emphasizes the importance of effective oversight of nonbank financial institutions (NBFIs) and calls for improved data collection, coordination and analysis, especially across borders. European authorities are scrutinizing private capital to boost transparency. In 2023, the Bank of England began "stress testing" NBFIs to understand how interactions with banks during stress could amplify shocks across markets. Following in its footsteps, EU authorities will carry out stress tests in 2027. Their outcomes open the possibility of heightened regulation and more disclosure around private capital.

In contrast to systemic risk where supervisors share the same approach, Europe is diverging over alternative investment fund (AIF) structures typically used by private capital. Both the UK and the EU are updating their regulation. The EU's reforms to its AIF Managers Directive or AIFMD2 come into force in April 2026. These will address gaps in the original directive and better align with market developments. There are new harmonized cross-border rules for AIFs engaging in loan origination to improve risk management for lending, including assessing credit risk and limits on leverage — where individual member states can impose stricter limits. More information will be required around delegation arrangements to third parties, as well as stricter substance rules on physical presence needed in the EU. The UK, meanwhile, is using its Brexit freedoms to create what it sees as a simpler, more proportionate framework for AIF managers. The number of funds, according to net asset value, subject to the full-scope regime will fall significantly. There is to be a consultation on the detailed rules in 2026. While UK reforms offer advantages, divergence from the EU poses a dilemma for fund managers, especially where they provide services to EU AIFs on a delegated basis.

In contrast to systemic risk where supervisors share the same approach, Europe is diverging over alternative investment fund (AIF) structures typically used by private capital. Both the UK and the EU are updating their regulation. The EU's reforms to its AIF Managers Directive or AIFMD2 come into force in April 2026. These will address gaps in the original directive and better align with market developments. There are new harmonized cross-border rules for AIFs engaging in loan origination to improve risk management for lending, including assessing credit risk and limits on leverage — where individual member states can impose stricter limits. More information will be required around delegation arrangements to third parties, as well as stricter substance rules on physical presence needed in the EU. The UK, meanwhile, is using its Brexit freedoms to create what it sees as a simpler, more proportionate framework for AIF managers.

The number of funds, according to net asset value, subject to the full-scope regime will fall significantly. There is to be a consultation on the detailed rules in 2026. While UK reforms offer advantages, divergence from the EU poses a dilemma for fund managers, especially where they provide services to EU AIFs on a delegated basis.

Private credit can sometimes struggle to finance projects, although co-lending alongside other private credit lenders may be a solution. Increasing consolidation between mid-market credit funds with deal expertise and pension or insurance funds with capital to invest should help. In future, the EU's revamped European Long-term Investment Fund and the UK's new equivalent — like interval funds — could create new funding sources, while both widening retail investors' access to alternative assets and making direct finance more readily available to SMEs.

Tokenization

Financial institutions need to familiarize themselves with the essentials of tokenization, and quickly. After fits and starts, momentum is building behind the development of markets in tokenized assets. These are not cryptocurrencies, but rather digital tokens linked to existing financial or physical assets that enjoy an increasing measure of legal certainty.

Today's main tokenized use cases are investment funds, shares and payments. The first, also known as blockchain-traded funds, are operated by large asset-management firms and digital start-ups. They are typically mutual funds where the shares or units are held as digital tokens registered on a blockchain.

Money markets have been the focal point of most tokenized fund activity attracting upwards of

USD 5 billion

(Moody's).

Investment managers and digital-native challengers have issued funds in US treasury bills that are collectively valued at over USD 8 billion (RWA.xyz). Increasingly, tokens tracking preexisting shares are tradeable on DiFi and other platforms. Efforts to use tokenized global depositary receipts to tap pre-IPO share markets have been announced. We may even see in Islamic finance tokenized sukuks. As for payments, these are digital representations of traditional bank-regulated deposits (e.g., bank accounts). The tokens are registered on a blockchain and can be used as payment for tokenized assets, including shares, interests in tokenized funds and other assets.

Tokenization offers investment funds efficiency gains and cost reductions in reduced workflows, such as maintaining investor registers. Another is disintermediation. As transactions increasingly take place on blockchains, there will be fewer third-party firms, thus offering efficiencies. This technology also allows for the creation of secondary markets in many assets, which should bring added liquidity to funds. Faster settlement, reduced risk of fraud (thanks to greater transparency) and new revenue models are other potential benefits (e.g., using tokenized money market funds as collateral in lending).

The full impact will be achieved when on-chain models that are managed fully or mostly on-chain become mainstream. However, there are obstacles. One is interoperability of technology platforms for tokenized assets. Different types of blockchain must operate to common standards to interconnect seamlessly. Another is regulation. Hybrid off-chain/on-chain funds are generally governed by existing securities regulation, but fully on-chain funds are not. Jurisdictions must resolve the legal frameworks that will govern these. Further, the fact that investor protection laws usually attach at the domicile or citizenship of investors remains a hurdle to the global distribution and tradability of asset tokens. For funds, international distribution may be even more complicated, as the strictest registration, licensing and investor protection rules tend to apply.

Tokenized assets' long-term growth also turns on innovation in payments. Stablecoins' weaknesses, including a lack of transparency over the reserves backing them, reduce their appeal as a currency. While CBDCs are underdeveloped, tokenized deposits offer the best near-term prospects for an on-chain payment medium. If adopted at scale, tokenized deposits will improve payments in several ways. One of those is atomic settlement, which ensures that transactions involving tokenized assets and deposits are executed instantly. Various financial regulators and central banks are supportive of tokenized deposits' potential and active in their development, such as the Monetary Authority of Singapore's Project Guardian and the Bank for International Settlement's Project Agorá.

Adoption at scale is not yet a given. A lack of platform interoperability is one reason. The benefits of implementation for any one financial institution are limited until others enter this space, while costs are significant given compliance and security requirements. Until then, many entities may stick with traditional payment systems, as, at least in OECD countries, banking systems work well in the transfer of money.

As the results of projects such as Agorá and Guardian become clearer, so too will the time frames for commercial adoption of this payment medium. More mature regulatory frameworks are being implemented such as Switzerland's DLT framework, the EU's Markets in Crypto-Assets Regulation, the recent US GENIUS Act and new Australian legislation. Regulators, while now generally more supportive,

need to clarify lingering areas of legal uncertainty. Questions remain, for example, over whether governmental protection for conventional deposits extends to their tokenized counterparts; over the legal enforceability of transactions involving tokenized deposits in the case of fraud or disputes; and how anti-money laundering laws apply. The challenge for the financial sector in 2026 lies in effectively balancing and integrating commercial, operational and legal considerations.



"More mature regulatory frameworks for tokenization are being implemented, such as Switzerland's DLT framework, the EU's MiCA legislation, the recent US GENIUS Act and new legislation in Canada and Australia."

Dr. Yves Mauchle
Partner, Zurich

Regional Spotlight



> **"The combination of Islamic finance principles and green/SDG-linked financing has created strong demand for "sustainable sukuk."**

Adil Hussain
Partner, Dubai

Islamic finance in the Middle East

The Islamic finance market in the Middle East is estimated at

USD 4.42 trillion

in 2025 and is expected to reach

USD 7.31 trillion

by 2030.

Sovereign and corporate sukuk markets were the backbone of activity in 2024 and 2025 was expected to see a slowdown in issuances. Notwithstanding the market's expectation, governments and large corporates tapped demand for longer-dated, Sharia-compliant funding, while a growing tranche of deals carried sustainability or "green" labels.

The combination of Islamic finance principles (which emphasize ethical investment and stewardship) and green/SDG-linked financing has created strong demand for "sustainable sukuk." Issuance of such instruments rose in the first half of 2025 with entities such as the Saudi Electricity Company, the UAE government and Qatar National Bank issuing ESG-compliant sukuk in infrastructure projects including grid modernization, clean water projects and low carbon buildings projects. ESG-linked sukuk are continuing to gain traction, accounting for around 44% of GCC sustainable debt.

Looking to corporate issuances, issuers including energy and national champions used Islamic bonds to diversify funding sources and attract DIFC/ADGM and international investors comfortable with Shariah structures, underlining sukuk's maturation as a mainstream financing tool. In 2025, large transactions drew notable oversubscription, reflecting robust demand for credit-grade, Sharia-compliant paper. More recently among financial institutions, Dubai Islamic Bank announced the successful international launch of a USD 1 billion sustainability-linked sukuk. We expect issuances to continue in 2026 based on the levels of demand seen in 2025 notwithstanding initial expectations for the year.

A notable shift in 2025 so far has been in the composition of the target investor base for sukuk. For example, the UAE Ministry of Finance launched the Islamic T-Sukuk program to strengthen the local financial market and provide open retail access to sovereign sukuk and offer low-risk Sharia compliant investment options at accessible investment levels. This effort complements secondary market development and helps support future corporate issuances.

On the innovation front, digital Islamic finance gained traction. Islamic banks and fintechs rolled out Sharia-compliant digital banking, robo-advice and wealth platforms, as well as tokenization pilots aimed at fractionalizing real assets and sukuk. Certain crypto exchanges in the UAE are also focusing on Sharia compliant products and trading and we look forward to further development in this space.

The Middle East's Islamic finance trajectory in 2026 should bring steady growth built on product diversity and stronger domestic markets. While key underlying challenges remain — including the need for standardization of Sharia interpretations, secondary market liquidity and harmonized regulation across jurisdictions — policy initiatives and private-sector innovation make the region well-positioned to sustain its leadership in global Islamic finance.

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

Baker McKenzie empowers clients to compete in the global economy. We provide comprehensive and practical legal advice that cuts through complexity with clear, actionable guidance. Our people represent diverse cultures and jurisdictions, combining local know-how with international expertise to ensure your business thrives across borders.

bakermckenzie.com

© 2026 Baker McKenzie. All rights reserved. Baker & McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Baker McKenzie.