Global AI Regulation Report

Executive Perspectives on the Emerging Global and Regional Regulatory Landscape

BRG

GLOBAL AI REGULATION REPORT
GLOBAL AI REGULATION REPORT
GLOBAL AI REGULATION REPORT
GLOBAL AI REGULATION REPORT

I. Executive Summary

Everyone is talking about artificial intelligence (AI)—but conversations often leave business leaders with more questions than answers.

This is especially true regarding ongoing debates over its regulation, which AI developers and business users alike are looking to for guidance. Perhaps Google's chief executive officer put the quandary best, remarking that "AI is too important not to regulate—and too important not to regulate well."

What would it actually mean to regulate AI well? That's a central question driving Berkeley Research Group's (BRG) 2024 *Global AI Regulation Report*. Drawing on responses from a survey of over two hundred corporate leaders and executive-level lawyers in diverse industries around the world—plus in-depth interviews with executives, attorneys, and BRG experts—we set out to evaluate where AI regulation stands, the challenges organizations face in complying, and what key stakeholders see as most important for the development of effective AI policy moving forward.

An Emerging Regulatory Landscape

Unsurprisingly, policy is very much in its early stages, with different jurisdictions' frameworks, guidelines, and requirements in varying stages of maturity—from the European Union's more risk-based AI Act and the Association of Southeast Asian Nations' (ASEAN) business-friendly *Guide on AI Governance and Ethics* to President Biden's executive order and myriad state- and country-specific laws now taking shape.

Given this patchwork, business leaders view the effectiveness of AI policy in different ways. Lawyers are far less confident in it than executives, as are North American respondents compared to those in Europe, the Middle East, and Africa (EMEA) and Asia-Pacific (APAC). Overall, only about one-third of respondents view today's policies as "very effective."

The emergent state of regulation creates risk—but also opportunity. "More and more, we're seeing a gap between what outside counsel recommends and what executives are open to when it comes to AI policies and procedures," says Amy Worley, a managing director and associate general counsel at BRG. "Good advisers can say yes, there is a lot of regulatory uncertainty, and where there is uncertainty there is also value."

"More and more, we're seeing a gap between what outside counsel recommends and what executives are open to when it comes to AI policies and procedures."

– Amy Worley
BRG, Washington, DC

TABLE OF CONTENTS

Lackluster Confidence in Compliance

There is room for improvement on the compliance front. Just four in ten respondents are highly confident in their organization's ability to comply with current regulations and guidance. The majority of respondents—and particularly those in the retail and consumer goods sector—have yet to implement internal safeguards to promote responsible and effective AI development and use.

Noncompliance or irresponsible AI use has consequences. Under the EU's AI Act, organizations could face fines amounting to up to 7% of annual global revenues. The still-maturing technology poses significant cybersecurity threats. Additionally, businesses risk losing customer or investor trust: in the past, the use of AI has drawn criticism from Hollywood writers and actors, consumers of retail brands like Levi Strauss (which used AI to generate images of more body-inclusive models), and judges who have caught lawyers filing ChatGPT-aided briefs replete with false information—not to mention ongoing intellectual property litigation against AI developers.

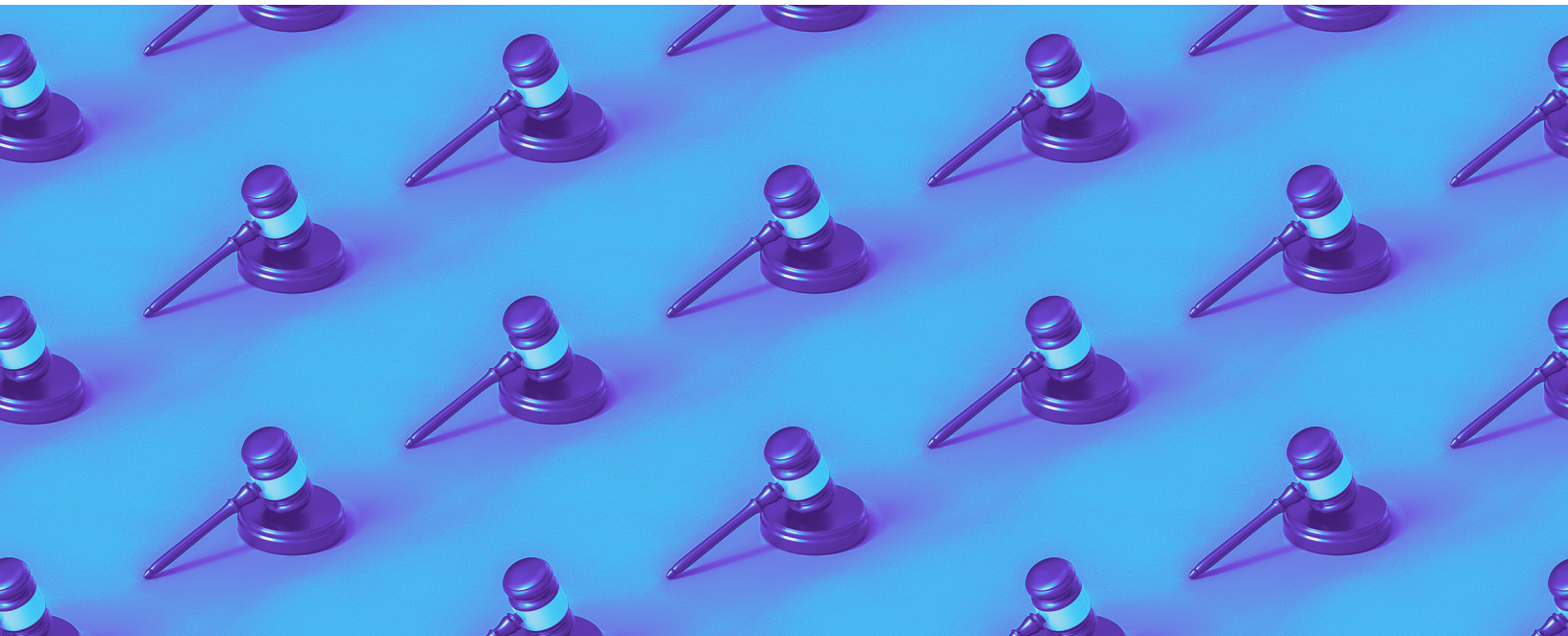
An Uncertain Future

Executives and lawyers agree that effective regulation will have to account for these and other factors, including data integrity, security, and accuracy, as well as complicated questions around liability. Importantly, respondents told us they largely want a broad, comprehensive approach rather than sector- or country-specific guidelines. While more than half expect effective AI policy (57%) within three years, only 36% feel strongly that future regulation would provide the necessary guardrails.

AI's ever-widening scope, rapid evolution, and technical complexity won't make regulators' jobs easy. As one of the organizers of the British government's 2023 AI Safety Summit put it, "There is a lot of good will … [but] we still don't know what the answer is."

Creating broad, comprehensive guidelines may prove more difficult than people imagine, adds Richard Finkelman, a managing director and artificial intelligence expert at BRG. "A fault line already exists between the US and EU over AI regulation and ethics—and it's getting larger."

We hope this report provides business leaders and their counsel with a firmer sense of today's policy landscape, where their organizations stand, and how to prepare for what's to come.



II. Key Findings

AI regulation is still emerging, and perceptions of its present effectiveness are mixed.

Lawyers are more cautious—and less confident—about regulatory effectiveness and compliance.

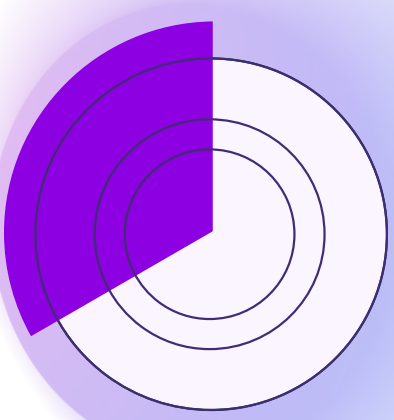
Attorneys, who are on the front lines when it comes to managing most AI-related risks, are understandably more skeptical than their executive counterparts when it comes to the effectiveness of current policy and their clients' abilities to comply.

Data integrity, security, and accuracy/reliability are the three main focus areas for regulators and businesses.

AI is only as good (or bad) as the underlying data. These were cited as main areas of compliance focus for organizations, as well as the most important for policymakers to address.

"Executives are trained to create value and think about finding the opportunity in the chaos. Lawyers are trained to identify and mitigate risk. Both ways of thinking are extremely valuable to any business."

– Amy Worley
BRG, Washington, DC

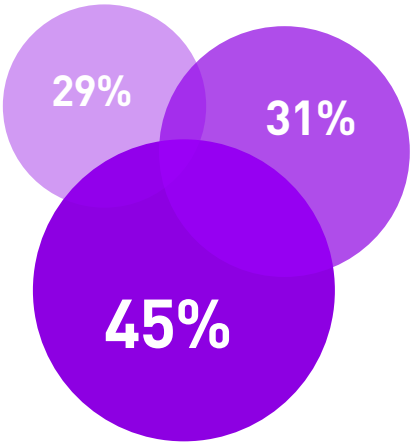


About one-third of respondents believe current policy is "very effective."

But roughly the same proportion believes it is "moderately effective" or a combination of "slightly effective"/"not effective."

Only four in ten are highly confident in their ability to comply with current regulation and guidance.

Respondents cite lack of internal training and inadequate data management/security protocols as primary reasons.



Less than half of all organizations have implemented internal safeguards to promote responsible and effective AI development and use.

The highest proportion of organizations (45%) have implemented data quality, collection, and storage reviews—as well as data protection, privacy, and security risk reviews—while less than one-third have implemented cross-functional teams to manage AI (31%) or processes to mitigate biases and ensure ethical use (29%).

Only 36% of respondents feel strongly that future AI regulation will provide necessary guardrails.

At the same time, more than half (57%) expect "effective" AI policy within three years.

"What we know about AI, ironically, is that we don't know enough. We have only scratched the surface when it comes to how we can handle regulation."

– Yuankai Lin,
RPC Premier Law, Singapore

III. Regulatory Outlook

Current Policy Effectiveness

"Embryonic." "A work in progress." "Ten years behind proper regulation." "Improving." "Very effective … so far."

These are just a few responses from survey takers asked to describe the state of AI regulation (see insert below for summary of key policies). Respondents exhibited a range of views that generally depend on their role, jurisdiction, and sector. Our survey reveals no clear agreement about the efficacy of AI regulation or what it should look like in the future.

Overall, respondents are fairly evenly split between current policy being "very effective," "moderately effective," or "slightly effective"/"not effective," with roughly one-third selecting each. Data integrity and ethics/morality were the two strongest areas of AI policy, with 34% of respondents saying existing policies are "very effective" in this regard.

Intellectual property (IP) and misinformation/deep fakes were cited as the least-effective areas of current policy. This should come as little surprise given ongoing IP-related litigation, complex questions about liability, and proliferating misinformation campaigns and deepfakes.

"We have to make sure that we are feeding the algorithms with things that have been approved and not infringing on other people's IP," says Steve Fraley, former global data protection officer at Vonage.

One notable deepfake example? An AI photo of an explosion near the Pentagon pushed US stocks lower after spreading on social media.

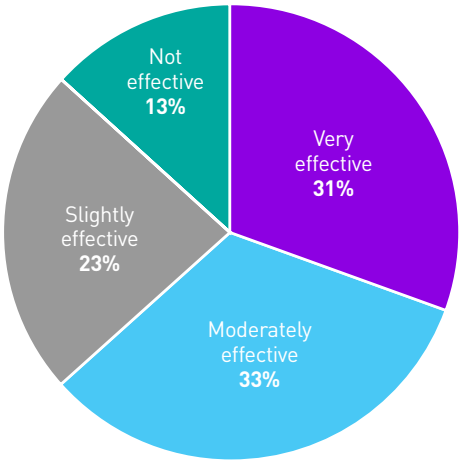
Broadly speaking, lawyers are more pessimistic than executives about current policy: more than double the share of legal respondents (22%) said current policy was "not effective," compared to just 10% of their executive counterparts. Respondents in the tech sector, meanwhile, are more optimistic (37% say current policy is "very effective," and only 5% say it is "not effective") than their counterparts in financial services and retail/consumer goods (17% and 13%, respectively, believe current policy is "not effective").

In-depth interviews with select executives and attorneys underscored these results.

As RPC Premier Law's Lin told us: "The market has moved on before we can wrap our head around how to monitor current GenAI capabilities." This was evident with the EU's AI Act, which originated in 2021, was passed in 2024, and has had to play catch up with generative AI. A 2023 Stanford University study, for instance, found that the most commonly used GenAI foundation models were largely not in compliance with the (then draft) act's requirements. Though the act evolved considerably prior to its final passing, the Stanford findings illustrate the ongoing challenges of regulating such a fast-evolving technology.

Michael Canale, a managing director at BRG, highlights the importance of adapting existing regulations like the General Data Protection Regulation (GDPR) and consumer protection laws that prohibit unfair or deceptive practices—particularly for financial services firms. "AI is disruptive and advancing rapidly, with new use cases emerging quickly. Companies need flexible and adaptable policies to incorporate these innovations without requiring a complete overhaul of regulations."

Effectiveness of current AI policy in addressing the development, deployment, and use of AI



BRG's Finkelman sums up the policy debate this way: "Do we need new regulations for generative AI, or do existing technology regulations already provide an appropriate framework for managing risk?"

Confidence in current policy also depends on where an organization operates. North American respondents are less confident than their peers in Asia-Pacific (APAC) and Europe, the Middle East, and Africa (EMEA), with just 28% believing AI regulation is "very effective" and 18% saying it is "not effective."

BRG's Worley says this lack of confidence likely stems from the fact that the US doesn't have a unified federal approach like the EU or APAC countries like China and South Korea. "North American companies that can implement an effective governance structure—perhaps one that combines EU and APAC approaches—will have a competitive advantage."

Summary of AI Policy Landscape

"The jury is still out about whether you can regulate this technology," said Andrea Renda, a senior research fellow at the Centre for European Policy Studies, a thinktank in Brussels.

That hasn't stopped governments, international bodies, and companies from trying. **The most comprehensive rules stem from the EU's AI Act, which the European Parliament passed in March 2024.** An interventionist, risk-based approach, the AI Act prohibits the use of AI for things like detecting emotions in workplaces and schools, limits its use in contexts like sorting job applications, and establishes restrictions on GenAI tools (recent reports suggest the UK is starting to draft regulations focused on the powerful language models underpinning ChatGPT).

Importantly, the EU law has extraterritorial reach, putting new compliance obligations on both providers that place AI systems on the market in the EU and deployers whose AI outputs are used in the EU—irrespective of where they're based. Already, French and German governments have critiqued the legislation, fearing it will impact AI startups in their respective countries and act as **barriers to innovation.**

"We are still a few years away from the EU AI Act really affecting everyday use of AI, assuming it's not high risk or prohibitive," says John Groom, a London-based partner at Baker McKenzie. "Yet we're still working out how the broadly drafted provisions will apply. It's probably fair to say that the act contains so much within it that it could be a barrier to startups being able to launch an effective product and get users on board."

On the other end of the spectrum, the **US government is following its traditionally decentralized, innovation-friendly approach**—though whether it succeeds in continuing to encourage innovation remains to be seen, given the fragmentary nature of the country's AI regulatory landscape. Though four major companies made voluntary commitments on AI safety following the White House's 2023 executive order, over a quarter of state legislatures are now considering legislation that would further regulate the private sector's use of AI—broadly related to algorithmic discrimination, automated employment decision-making, an AI bill of rights, and/or "working group" bills.

In lieu of overarching federal regulation, **US regulatory bodies likely will apply sector-specific rules** and guardrails: for instance, the Federal Trade Commission (FTC) approved an omnibus resolution authorizing the use of compulsory process in nonpublic investigations involving products and services that leverage AI; and the Food and Drug Administration (FDA) released guidance related to the development of medical products and completed a pilot program examining new ways to certify AI systems.

These developments are inevitable given the inherent risks in AI advancement and deployment and the regulatory vacuum. As Paul Scharre and Vivek Chilukuri of the Center for a New American Security wrote in an op-ed for *Time*, "**Cryptocurrency offers a cautionary tale.** The virtually unregulated sector resulted, predictably, in the spectacular implosion of FTX … It is not hard to imagine unregulated AI applications producing an equally high-profile failure that could hinder adoption or lead to a regulatory overcorrection from Washington. **To run far, AI must run safely.**"

Demographic breakout: Effectiveness of current AI policy in addressing the development, deployment, and use of AI

	POSITION		INDUSTRY			REGION		
	Executives	Lawyers	Financial services	Retail and consumer goods	Technology	APAC	EMEA	North America
Very effective	32%	26%	36%	26%	37%	31%	31%	28%
Moderately effective	32%	27%	25%	31%	39%	33%	33%	27%
Slightly effective	23%	23%	21%	25%	19%	25%	21%	24%
Not effective	10%	22%	17%	13%	5%	9%	12%	18%

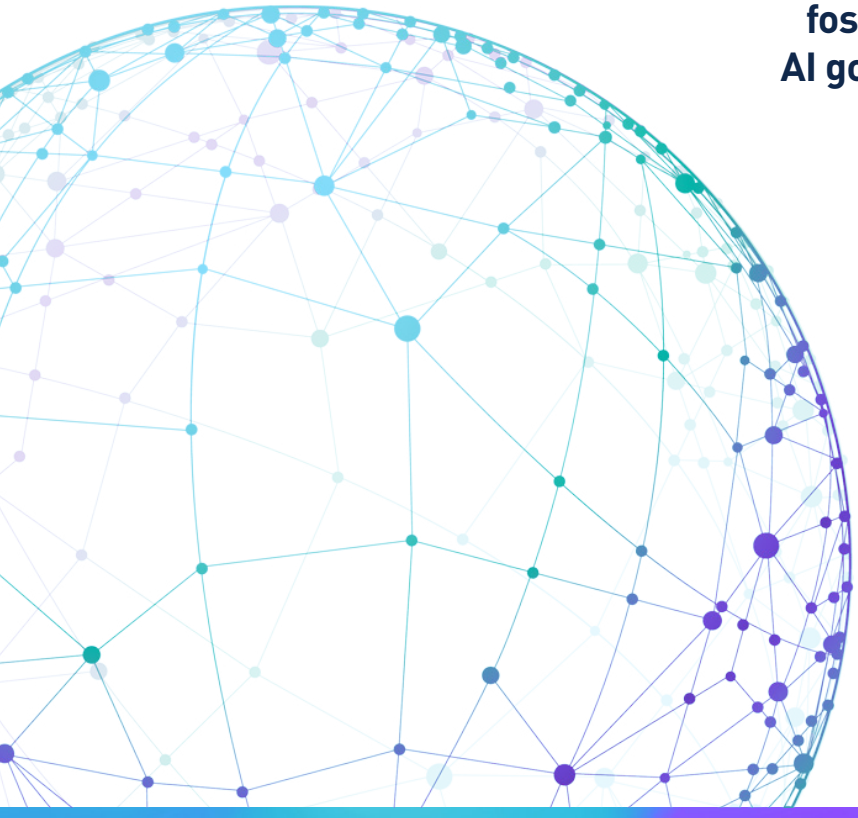
Between these two poles, **business and civil society groups have advocated for their own measures.** Microsoft's *Governing AI: A Blueprint for the Future*, for instance, calls for creating a new government AI agency and new AI legal framework and for requiring safety controls for AI systems that run critical infrastructure, among other actions.

Meanwhile, APAC countries have taken a varied approach, from China's regulations—which are focused on state control—and South Korea's comprehensive legislation to Australia and Singapore's more hands-off guidance. The region's policies are stimulating innovation and economic growth, yet many countries still lack regulations to address ethical concerns, data privacy and security, and inequality caused by AI-driven automation, says Erick Gunawan, a Singapore-based managing director and head of BRG's Cyber Forensics and eDiscovery practice in APAC.

Certain governments worldwide, like the United Arab Emirates and Saudi Arabia, are pouring funds into AI research. **In Africa, China and the US are "in a new race to shape the development, use, and governance of artificial intelligence** … even as African countries scramble to devise their own AI policies," according to *Semafor*, which cites an American deal with Kenya to invest in AI data centers.

Overlaying more country- and sector-specific policies, international forums and collaboratives have put forth their own frameworks and working groups, including the Hiroshima Process, which established a framework for the G7 to discuss the use and regulation of generative AI; the United Nations AI Advisory Body; the Santiago Declaration, signed by twenty Latin American and Caribbean nations, which intends to promote the responsible and ethical use of AI; and the Association of Southeast Asian Nations' (ASEAN) *Guide on AI Governance and Ethics*, which provides a comprehensive framework for member states to develop AI policies and regulations and harmonize standards.

"The ASEAN *Guide* adopts a business-friendly approach that prioritizes innovation and flexibility, while the EU's AI Act sets high standards for accountability and transparency with a clear legal framework," adds Gunawan. "The pros and cons of these differences highlight the trade-offs between promoting innovation and protecting against potential risks associated with AI deployment. Finding the right balance between fostering innovation and ensuring ethical AI governance remains a key challenge for policymakers around the world."



"Finding the right balance between fostering innovation and ensuring ethical AI governance remains a key challenge for policymakers around the world."

– Erick Gunawan
BRG, Singapore

The Risk of Noncompliance

The risks of noncompliance—with both current AI law and existing regulations—are steep and getting steeper. "There is very little AI case law," says Finkelman, "but that is about to change, and it will happen quickly."

AI technology disputes, he adds, will lead to new case law, while failure to properly identify and handle AI data will lead to new precedent, as in Judge Scheindlin's groundbreaking opinion in *Zubulake v. UBS Warburg* and Judge Peck's opinion in *Da Silva Moore v. Publicis Groupe et al.* Those cases had more influence on codifying the Federal Rules of Civil Procedure regarding the proper handling of electronic information than any policies or best practices. "Sometime in the next eighteen to twenty-four months," Finkelman says, "a new precedent-setting case will start a similar process for codifying AI electronic discovery rules."

For now, examples of regulatory penalties and litigation in key industry sectors include:

Financial Services

- **CFPB fines fintech for defective finance algorithm.** In 2022, the Consumer Financial Protection Board imposed a $2.7 million fine on Hello Digit, a fintech company that promotes automated savings, for using an algorithm that led to overdrafts and penalties.
- **Germany fines bank for lack of transparency around automated credit card application system.** The Berlin Data Protection Authority fined a Berlin-based bank for not informing a credit-card candidate of the reasons behind an automated rejection for their online application. This was in violation of articles 22(3), 5(1)(a), and 15(1)(h) of the GDPR, which cover automated individual decision-making, lawful and transparent processing of personal data, and right of access by the data subject.

Technology

- **Eight US newspapers sue OpenAI for copyright infringement related to AI training.** In April a group of newspapers including the *Chicago Tribune* and *New York Daily News* *filed* a suit against Microsoft and OpenAI in New York federal court, alleging the companies unlawfully copied articles to train their generative AI systems. This complaint follows other lawsuits brought by *The New York Times* and *other* outlets; meanwhile, in France, competition authorities fined Google $271 million for training Bard AI on news articles without giving publishers sufficient information about renumeration or opportunities to opt out.
- **Ireland fines Meta for lack of transparency around data processing.** In December 2022, the Irish Data Protection Commission fined Meta Ireland €390 million for breaches of the GDPR. Both Facebook and Instagram were found to be using profiling, behavioral advertising, and algorithms without adequately informing users. Several big tech companies have faced similar GDPR-related fines for data-driven ad targeting without proper consent.
- **US class action alleges collusion via use of AI software's algorithmic pricing.** The proposed class action from renters claims that dozens of landlords gave price-setting authority to RealPage Inc., a software company whose tool analyzes landlord-supplied data on pricing and leasing for apartments. As *Bloomberg Law* notes, "The case will show how decades-old antitrust laws might govern price-fixing suits involving algorithmic databases that crunch massive amounts of competitive information far faster than a group of humans ever could."

Retail

- **FTC prohibits use of facial recognition technology in Rite Aid stores for five years.** Last December, the FTC delivered an enforcement action against the large US retailer, claiming it had failed to implement reasonable procedures while deploying AI-based facial recognition technology.
- **Royal Mail fined for nonconsensual automated marketing.** In 2022, the UK's Information Commissioner's Office fined Royal Mail for using an AI-powered tool that sent emails to customers who had opted out of receiving them.
- **Fashion giant Shein sued for copyright infringement, data scraping, and using AI to steal art.** The class-action suit "alleges that the company uses data scraping and electronic monitoring to identify popular designs and steals them to generate its products."

CONTINUE TO PAPER >

The Future of AI Regulation

Given today's still-developing AI policy landscape and the rapid pace of the technology's evolution and adoption, respondents expressed a wide range of perspectives regarding future regulation.

Just over one-third (36%) strongly agree future regulation will provide necessary AI guardrails, while 42% somewhat agree, 13% neither agree nor disagree, and 10% disagree. Of the 78% who agree to some extent, most (62%) believe regulation will be in place in the next one to three years; 24% believe it will take four to six years, and 11% believe it's already in place.

"AI regulation is in a very dynamic phase, and the level of development and sophistication varies significantly across geographies and regions," says Richard Allen, a Singapore-based local principal at Baker McKenzie. "We anticipate that it will become far more stringent over the medium term."

Given the divergence across regions, it tracks that respondents from different jurisdictions also express varying levels of confidence in *future* policy. As with present regulation, North American respondents are far less confident than their counterparts in APAC and EMEA that future regulation and guidance in their jurisdiction will provide necessary guardrails: only 24% say they "strongly agree," compared with 45% of APAC respondents and 36% from EMEA.

Worley believes this reflects differences in legislative practices among the regions. The US historically has taken a decentralized, industry-specific approach with a robust private litigation component that can leave the country's businesses experiencing the scheme as fractured. Meanwhile, APAC and EMEA tend to favor a centralized and unified approach.

Yet there may be room for optimism in North America.

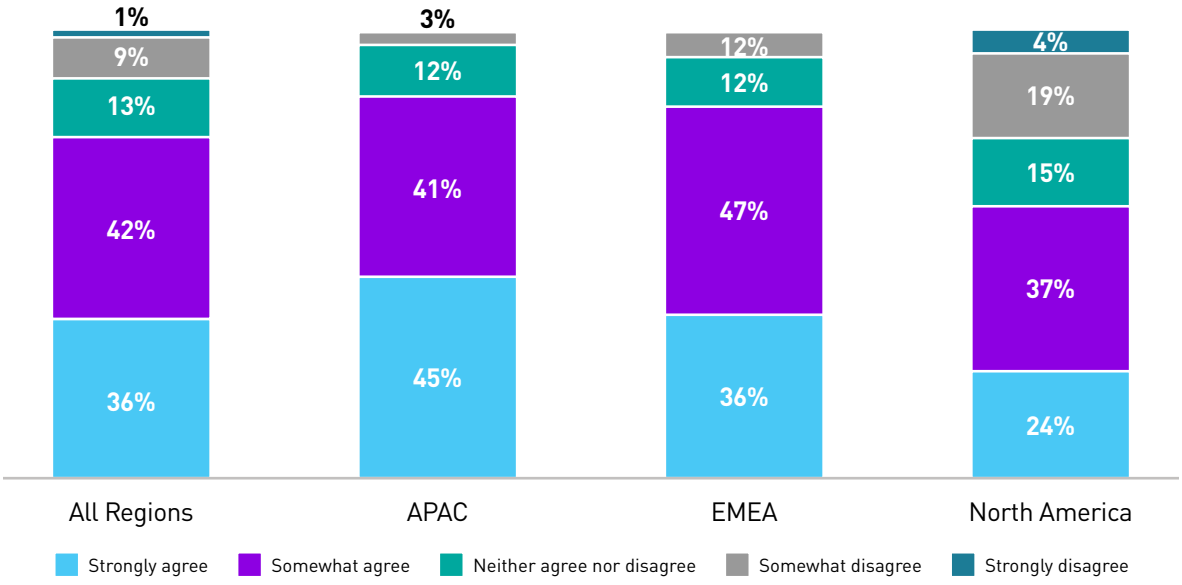
"There is a sense that legislators and regulators missed the window of influence with big tech, and they are trying not to do that with AI," Worley says. "This means regulatory efforts in North America are moving faster than usual. Though it is an election year, technology regulation is becoming an increasingly bipartisan issue, and I expect legislative action in the next one to three years. The shape of that legislation, however, will very much depend on who is in control politically."

Similarly, technology respondents are more confident (47% "strongly agree" future regulation will provide necessary guardrails) than those in retail and consumer goods (20%) and financial services (18%).

Finkelman attributes technology respondents' optimism to their familiarity with AI. "If you know how to build something, you inherently know more than those who don't know how to build things."

Retailers' skepticism may stem from a long history of slow technology adoption in the sector. "The retail industry has a track record of getting excited about emerging technology, be it big data, blockchain, or RFID," says Murali Gokki, a managing director at BRG and co-leader of the firm's Retail Performance Improvement practice. "RFID, for instance, is finally catching on, but it took twenty years to get any traction and delivered just a fraction of what was initially promised."

Level of Agreement: "I feel confident future regulation and guidance in my jurisdiction will provide necessary guardrails for effective development, deployment, and use of AI."



More agreement emerges regarding future policy. When asked about characteristics policymakers should prioritize when establishing a framework for responsible development, deployment, and use of AI, roughly half of respondents selected comprehensive (50%), enforceable (48%), adaptable and flexible (47%), transparent and explainable (46%), and clear legal implications for misuse (45%).

Lawyers were most concerned about policy being enforceable, while executives focused on it being adaptable/flexible and transparent/explainable. This tracks with each role's priorities, says BRG Managing Director David Parker. "Executives are concerned about regulation that impacts their ability to develop new products, so are likely more focused on characteristics like adaptability, flexibility, and explainability. Lawyers, on the other hand, are concerned about how they can best help their clients ensure compliance and navigate the enforcement landscape as regulation emerges."

Less than a quarter of respondents selected sector-specific (24%), country-specific (21%), and company revenue or size thresholds (13%)—though for some these approaches may have benefits.

"The advantage of sector-specific responses is that, in many cases, you won't need to do anything," says Ben Allgrove, a London-based partner at Baker McKenzie. "So, if the concern is biased AI datasets creating discriminatory outcomes in mortgage approvals, the financial services sector doesn't need any new regulation because those biased outcomes are already prohibited."

Alternatively, Adam Rouse, senior counsel and director of e-Discovery Operations at Walgreens, thinks a national policy would be more effective. **"When we regulate sector by sector or try and segment regulations, we fall into this kind of trap where we get companies that have multiple functions—an insurance company, for instance, could fall under the healthcare or finance umbrella. Then you run into this problem where you pick whichever industry is most favorable to you and say, 'This is what we are in AI, but this is what we are in Sarbanes-Oxley.'"**

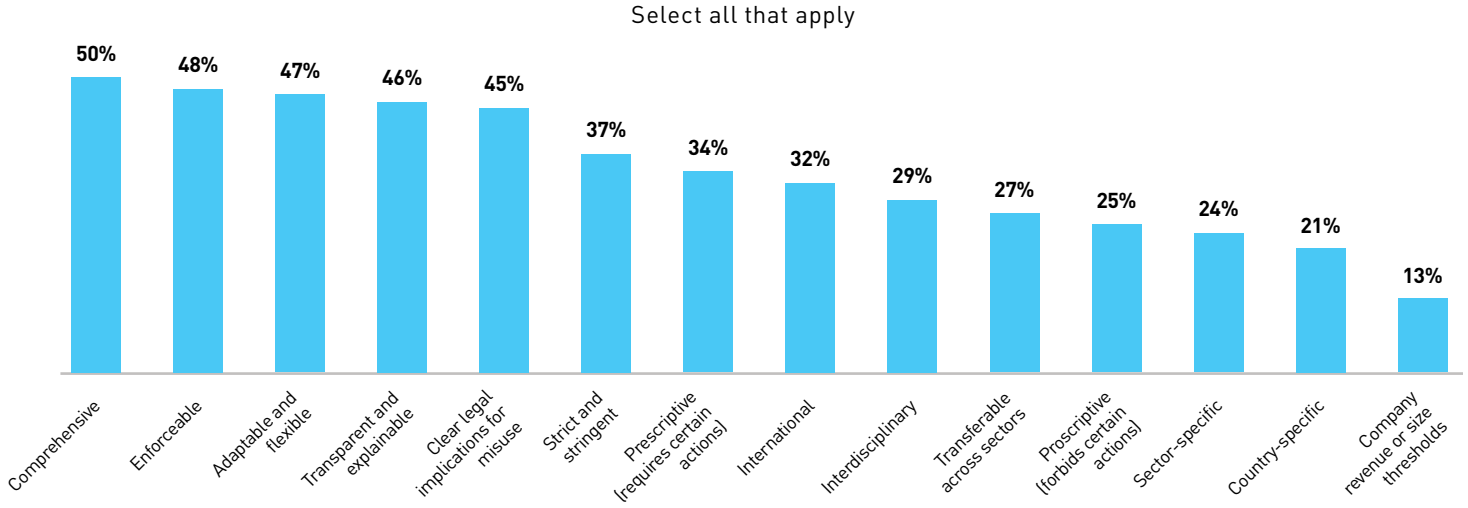
Divergences did occur, however, depending on respondent sector and jurisdiction. North Americans, likely anticipating a growing wave of AI-related litigation, are significantly more concerned about "clear legal implications for misuse" than policy being adaptable/flexible and transparent/explainable. APAC respondents are more used to and comfortable with sector- and country-specific regulations than their North American and EMEA counterparts. And EMEA participants, many of whom are already subject to comprehensive cross-border regulation, expressed more interest in AI policy being international (38%) and transferable across sectors (29%).

"Different industries are going to create their own [AI policies], and it's already happening," says RPC Premier Law's Lin. "For example, in Singapore, we already have some sector-specific guidance around autonomous vehicles and the financial industry because those are considered to be high-risk industries, inherently."

Financial services and technology respondents care deeply that future policy be adaptable and flexible, and nearly half of the former want prescriptive rules. Retail and consumer goods respondents, by contrast, are most focused on regulation being comprehensive (42%) and strict (42%).

"Financial services firms already have data analytics requirements, and they have to do so much with that data that it makes sense they want more adaptability and flexibility," says Worley.

Characteristics policymakers should prioritize when establishing a regulatory framework for responsible development, deployment, and use of AI.



CONTINUE TO PAPER >

AI and the Future of Healthcare

AI technologies are already transforming healthcare by speeding up clinical trials for life-saving drugs, providing personalized communications and treatment plans, improving administrative functions, and any number of other use cases. In the next five years, widescale adoption could lead to hundreds of billions of dollars in savings on US healthcare spending alone, according to the National Bureau of Economic Research.

Earlier this year, BRG's *AI and the Future of Healthcare* survey report gathered insights from more than 150 US healthcare provider and pharmaceutical professionals. The findings, when compared to those of this report, provide a unique snapshot of where the healthcare industry is headed.

US healthcare providers are bullish on current regulatory effectiveness, but pharmaceutical companies are less so. Six in ten healthcare providers agreed that current regulation provides the necessary guardrails for proper implementation and use of AI—roughly in line with this survey's financial services and retail respondents who said current regulation is moderately or very effective (tech respondents were even more bullish). Yet only 34% of pharmaceutical professionals said the same, perhaps a result of regulators struggling to keep pace with innovation in this area.

Looking ahead, however, most professionals—75% of provider respondents and 56% of pharmaceutical professionals—felt confident that future regulation and guidance will provide necessary guardrails for proper implementation and use of AI.

Compliance confidence for US healthcare and pharmaceutical organizations is high (~90%)—despite only four in ten saying they are reviewing or planning to review AI regulatory guidance. These results align with the findings in this report, which show a high degree of compliance confidence, even without many internal safeguards in place.

Cybersecurity/data management is a top concern. Nearly 70% of pharmaceutical professionals and 56% of provider respondents named cybersecurity/data management as their top concern when it comes to regulatory compliance and litigation exposure. Again, this mirrors global respondents' concerns around data protection, privacy, and security—though healthcare organizations have unique challenges in this area, largely related to potential violations of patient trust. This has led to the US Department of Health and Human Services releasing specific guidance on data privacy for AI use.

"AI is no longer an academic discussion or a dinner topic. C-suites and boards of directors across the healthcare sector have to identify which areas of AI will be the most impactful, understand implementation timelines, and have the self-discipline to fund the education process around this swiftly evolving technology."

—Tom O'Neil
BRG, Washington, DC

Effective AI Starts with Good Data

In establishing an effective regulatory framework, a clear theme emerged: the importance of good data. Among the most important principles for policymakers to address, respondents cited data protection, privacy, and security (66%), accuracy and reliability (60%), and data integrity (60%). Accountability and ethical use weren't far behind, while just over 40% of respondents selected transparency and equity/fairness.

The principles identified here are natural; AI systems and their outputs are only as good (and safe) as the data they run on. Big technology players are taking note: as *The New York Times* recently reported, "2024 is turning out to be the year of AI plumbing," with Microsoft, Meta, and Alphabet having spent over $30 billion combined on "data centers and other capital expenses" in the first three months of the year.

Importantly, these three areas—data protection, privacy, and security; accuracy and reliability; and data integrity—were also cited as the most important areas for policymakers to address—and, as we'll see in the next section of this report, the most challenging areas for companies.

Some policymakers are heeding the call. Worley notes that in the US, "There have already been bipartisan discussions in Congress of legislation around a framework focused on security, accountability, values-based foundations (e.g., liberty, democracy, free speech), explainability, and innovation. As these conversations continue and legislation is drafted, I expect we will see one or more risk-based laws built around a basic framework that incorporates these pillars."

Several respondents and interviewees expressed similar sentiments around future policy: "Regulate the risk, not the technology," says one survey taker. Others emphasize data protection and humanistic approaches that "balance innovation with responsibility." Still others underscored the importance of collaboration and reaching agreement on common definitions of what AI actually is.

That may be easier said than done. "I think it's going to be very difficult to come up with a global framework anytime soon," says Baker McKenzie's Allen. "If we're going to get to some kind of global agreement on how to regulate AI, it's going to be in line with the lowest common denominator, which won't really mean anything."

Governments also have their own perspectives on who should do the regulating: as *The Economist* notes, "America and Britain think existing government agencies can do most of the job. The EU wants to create a new regulatory body. Internationally, a few tech executives now call for the creation of something akin to the Intergovernmental Panel on Climate Change."

Finally, some expert commentators point to creative technological solutions. Andrew Burt, managing partner of Luminos.Law, a boutique law firm focused on AI and analytics, wrote in the *Harvard Business Review* that we should take lessons from the FDA's pilot program about how to certify AI systems—namely, that initiatives could be "centered on certifying processes surrounding software development rather than certifying each system itself." Researchers at AI company Anthropic, meanwhile, are pioneering "constitutional AI," which enables one AI system to supervise the content of another.

Most important principles for policymakers to address when establishing a regulatory framework for responsible development, deployment, and use of AI

Select all that apply

CONTINUE TO PAPER >

AI, Fake Evidence, and the Legal Industry

Recent headlines have highlighted fictitious case law generated by ChatGPT—but the more serious problem may be the rise of fake *evidence*.

"The potential for using generative AI to create deepfakes or alter documents poses risks to the credibility of evidence, a cornerstone of fair arbitration," says Elizabeth Chan, an international arbitration specialist with Stevenson, Wong & Co. "The risk is acute, especially given the potential for creating undetectable fake documentary, photographic, audio, or video evidence. Traditionally, the authenticity of documents could be verified by examining native files and their metadata. However, the sophistication of generative AI means that such deductive work has become significantly more challenging."

BRG's Gunawan notes that mitigating these risks requires a comprehensive approach combining technological solutions, procedural safeguards, and ethical considerations. His best practices include:

- **Implement robust authentication measures:** Use advanced technological tools such as blockchain or cryptographic techniques to authenticate digital evidence. These methods can help ensure the integrity and authenticity of data presented during legal proceedings.
- **Vet evidence thoroughly:** Establish stringent protocols for verifying the authenticity of evidence, particularly digital evidence generated or manipulated by AI algorithms. This may involve conducting forensic analysis and engaging consulting expert witnesses with specialized knowledge in AI and digital forensics.
- **Educate employees and stakeholders:** Provide comprehensive training to employees and stakeholders on the risks associated with AI-generated fake evidence and the importance of maintaining ethical standards in legal proceedings. Foster a culture of integrity and transparency within the organization.
- **Implement internal controls:** Develop internal policies and procedures for the collection, preservation, and presentation of evidence to ensure compliance with legal and ethical standards. Implement checks and balances to prevent the creation or dissemination of fake evidence within the organization.
- **Collaborate with external experts:** Engage with external experts, including legal professionals, technologists, and ethicists, to stay informed about emerging threats and best practices for managing fake evidence. Collaborate with academia, industry partners, and regulatory bodies to address complex ethical and legal challenges.
- **Stay vigilant and adapt:** Continuously monitor developments in AI technology and evolving legal standards to anticipate and mitigate emerging risks related to fake evidence. Regularly review and update internal policies and procedures to reflect the latest advancements and regulatory requirements.

IV. Organizational Readiness

Compliance Confidence

Is your organization ready to comply with current AI regulation and guidance?

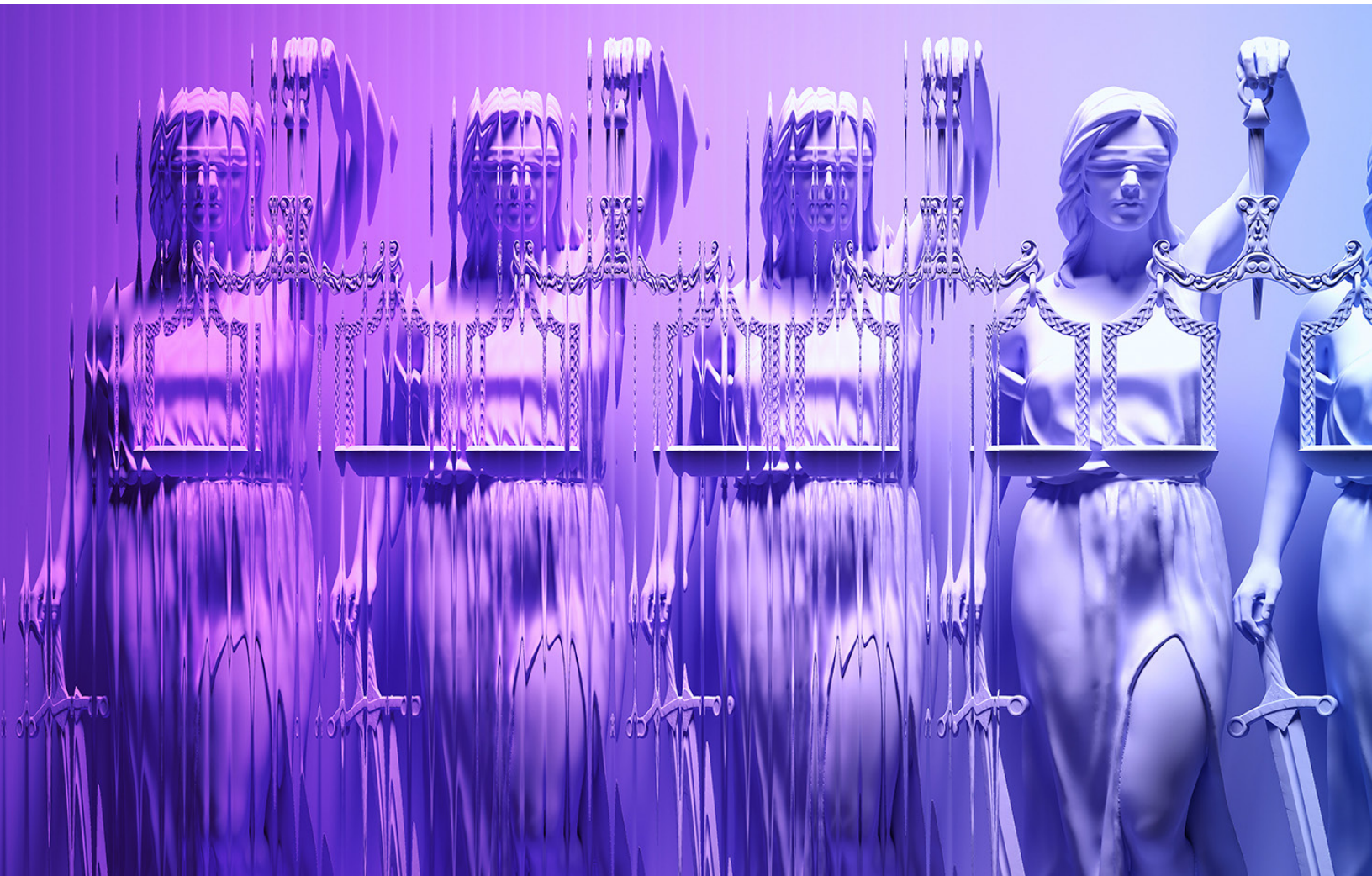
Most of those we surveyed say they are somewhat confident in their organization's ability to do so (91%). But, unsurprisingly given how fast the goalposts are moving, only four in ten are "very confident."

Those who are not confident cite lack of internal training or knowledge (61%) and inadequate data management and security protocols (50%) as top reasons, followed by lack of personnel dedicated to compliance (39%) and interdepartmental silos (33%).

Worley has seen these challenges firsthand: "My soapbox at the moment is that companies need to set up multidisciplinary teams to address AI compliance. Silos are simply not going to work."

"Imagine me standing on my big, wooden box," she says, "with a huge megaphone shouting, 'IT, InfoSec, Product, Data Science, Compliance, Legal, gather round, we need to solve really hard problems together!' Smart teams can shift with the goalposts, but it is going to take a lot of different talents and skill sets to maintain flexibility."

Just 4 in 10 organizations are very confident in their ability to comply with current AI regulation and guidance



Organizations Have Yet to Implement Key Internal Safeguards

Other respondents underscore the importance of treating AI as a governance issue. Yet the majority of companies we surveyed have yet to implement key internal safeguards to ensure the responsible and effective development and use of AI.

Of those safeguards, "data quality, collection and storage reviews" and "data protection, privacy, and security risk reviews" led the way (each implemented by 45% of respondents' organizations)—echoing the significance of good data referenced throughout this report. Cross-functional teams (31%) and processes to detect and mitigate biases and ensure ethical use (29%) ranked lowest in terms of implementation.

Nearly 60% of financial services companies, which are subject to greater regulatory scrutiny than other sectors on issues like data privacy, say they have internal safeguards around data protection, privacy, and security already in place. Over half of the technology respondents we surveyed have implemented data quality, collection, and storage reviews (51%)—likely because this is central to many of their companies' business models—as well as employee training (53%). Less-regulated retail and consumer goods organizations tended to lag behind, with less than one-third having implemented the majority of safeguards we asked about.

Data protection, privacy, and security; data integrity; and accuracy/reliability are the top three areas respondents expect to be the most challenging to address for establishing proper protocols and complying with future policy. Fittingly, organizations say they are most focused on these three areas for establishing protocols.

Our interviewees offered further explanations for why this might be the case. "Our customers are frequently telling us, 'We don't want you to use AI on any of our products or services,'" says Fraley. "But how do you harvest AI if you aren't allowed to use it on your customer data?"

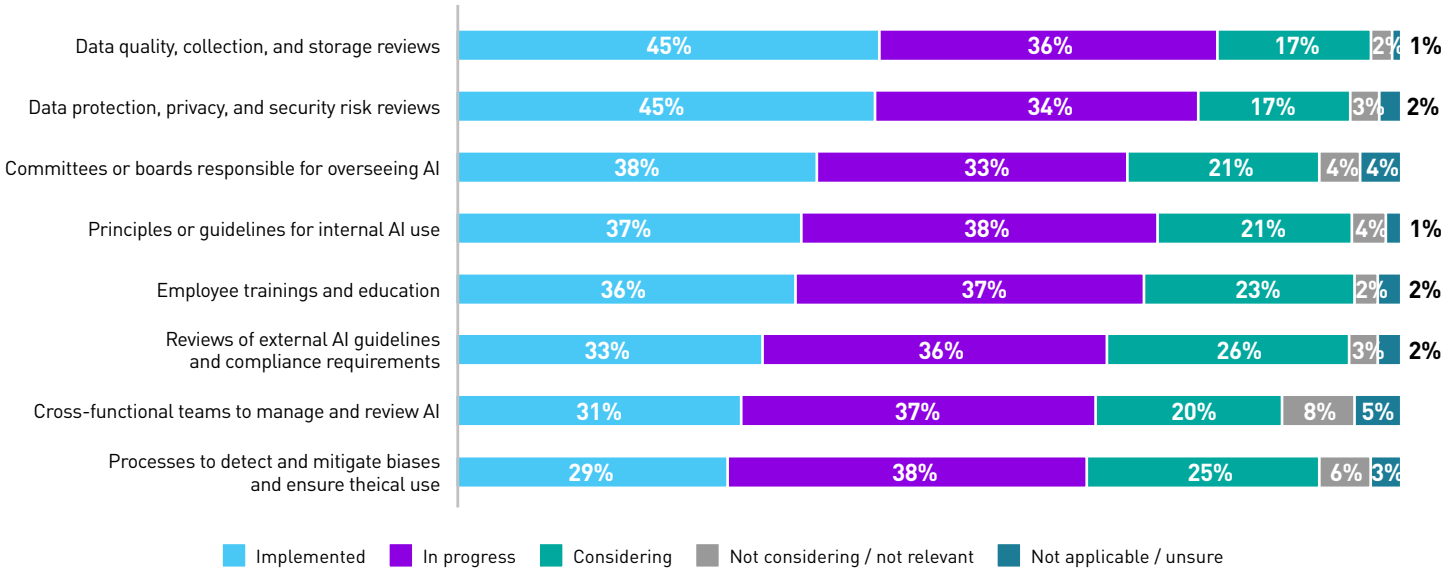
They also offered potential solutions. "Apply the most stringent frameworks and work backward," says Byron Phillips, a Hong Kong-based partner at Hogan Lovells. "That is not always seen as commercial. But it is important to have the tools to be compliant, and then you can loosen and innovate accordingly."

Similarly, Shawn Ashworth, a managing director and co-leader of BRG's Retail Performance Improvement practice, advises retailers just getting AI capabilities off the ground: "Don't pick the hardest area, like an AI-driven product selection engine, as your starting point. Start in customer service or by automating some low-level back-office functions. Then, as you build your expertise and confidence, continue to expand based on lessons learned."

On that front, Worley advises global organizations to advance by finding common principles and themes and building systems with those big ideas in mind.

And remember it's not a one-and-done. "It's not just about doing the risk assessment and putting it in the drawer," says Baker McKenzie's Allgrove. "It's revisiting the risk assessment, and at certain iterations over time, as the technology and compliance landscape evolves."

Implementation status: Internal safeguards for the responsible and effective development, deployment, and use of AI



V. Conclusion

AI is here to stay: the generative AI market alone is expected to surpass $1 trillion in the next decade.

Regulation will play a critical role in what these next ten years of AI will look like. And while some are rightly concerned that regulation will stifle innovation, other executives may *want* effective AI policies in place.

"Businesses that are looking to develop AI want it to be properly regulated," says Hogan Lovells' Phillips. "They want it to operate in an environment where the human endeavor is advanced through AI, where safe innovation is the goal. I don't worry that innovation will be stunted by ethics and governance; ethics and governance free them up to innovate within respectable parameters."

Getting there, however, will require extensive collaboration, agility, and flexibility across sectors, governments, and international bodies—which must agree on not only *how* but also what they're regulating. "As an initial step, regulators need to talk to one another, at a global level, to try and agree on a common base-level taxonomy, so at least we're all talking about the same thing," says Baker McKenzie's Allen.

Finally, executives and their legal counsel are seeking to implement safeguards and compliance protocols to mitigate burgeoning AI risk—finding answers to the many questions the technology invites. Companies that do so can mitigate reputational and financial harm and gain a distinct competitive advantage in the exciting years to come.

"As an initial step, regulators need to talk to one another, at a global level, to try and agree on a common base-level taxonomy, so at least we're all talking about the same thing."

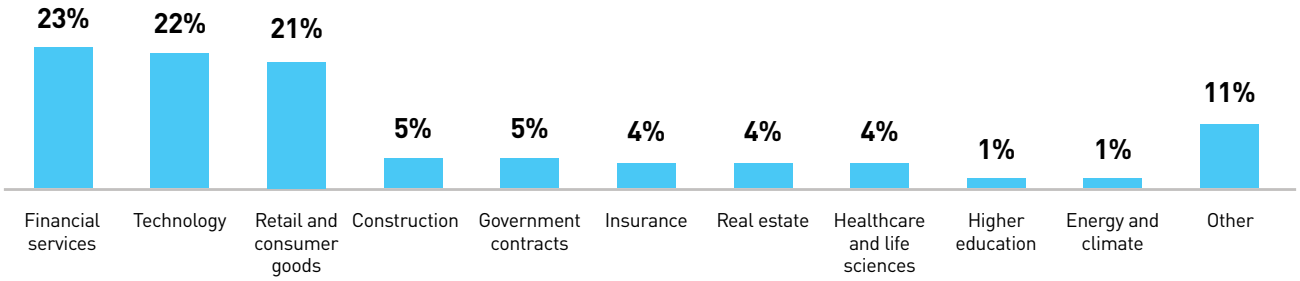
– Richard Allen
Baker McKenzie, Singapore

VI. Methodology

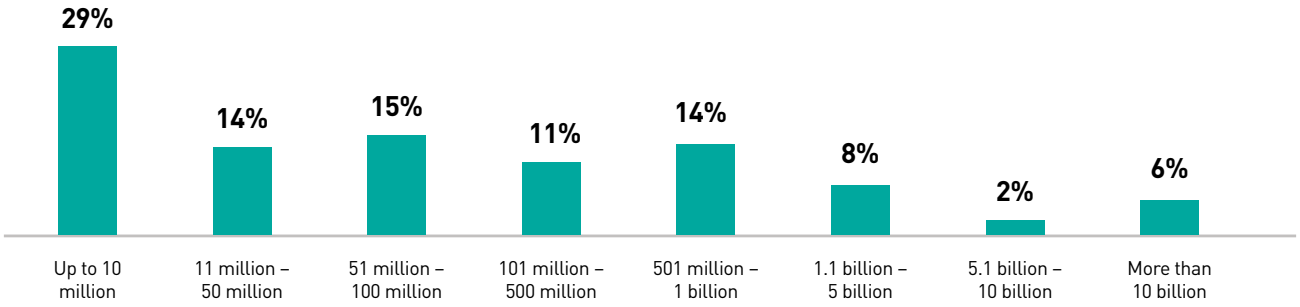
BRG surveyed 214 corporate leaders and executive-level lawyers across the globe in a diverse set of industries, with sizable participation in financial services, technology, and retail and consumer goods. Respondents held leadership positions at their organizations or firms; and had knowledge of or involvement in their organization's AI implementation status and/or advised clients on the implementation of their AI efforts.

The online survey was conducted in March and April 2024 with help from multiple panel providers. Responses are anonymous, and data was analyzed in the aggregate. Due to rounding as well as multi-selection questions, some totals may not add up exactly to 100%.

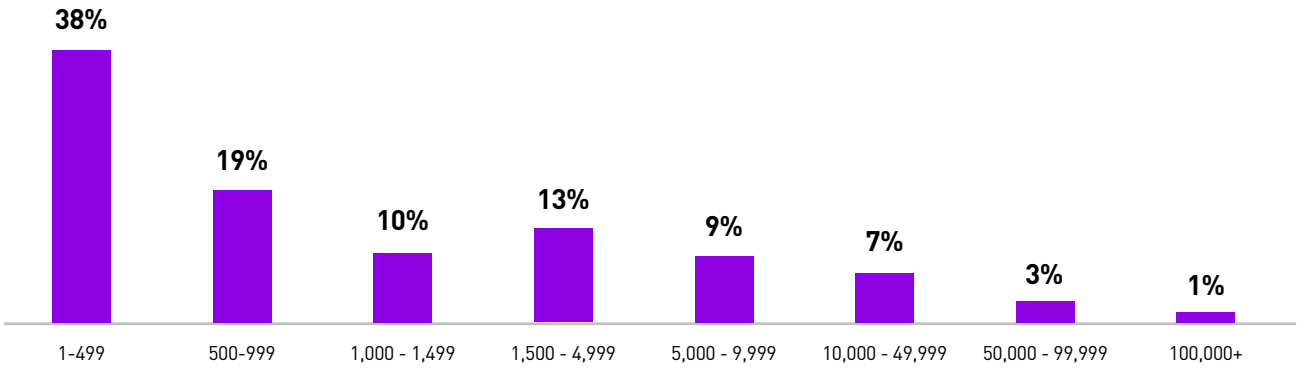
Which best defines your industry?



What was your organization's approximate 2023 gross revenue in USD?



How many employees does your organization employ?



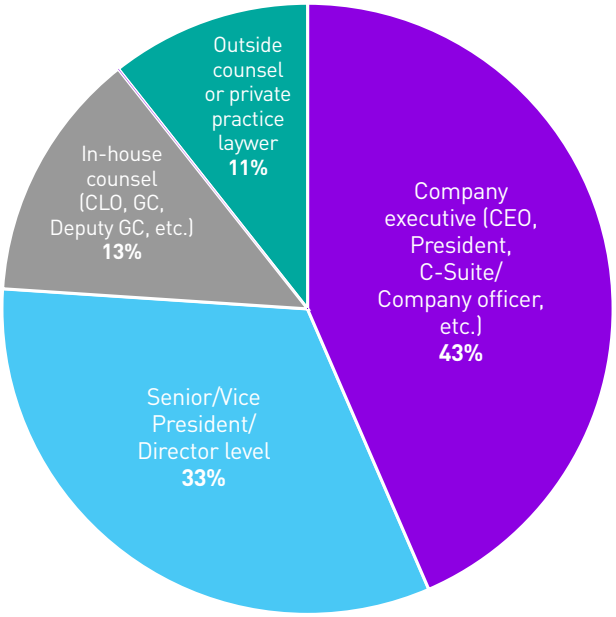
VII. Demographics

In the report, which draws on the responses of 214 corporate leaders and executive-level lawyers, we segment data into various categories:

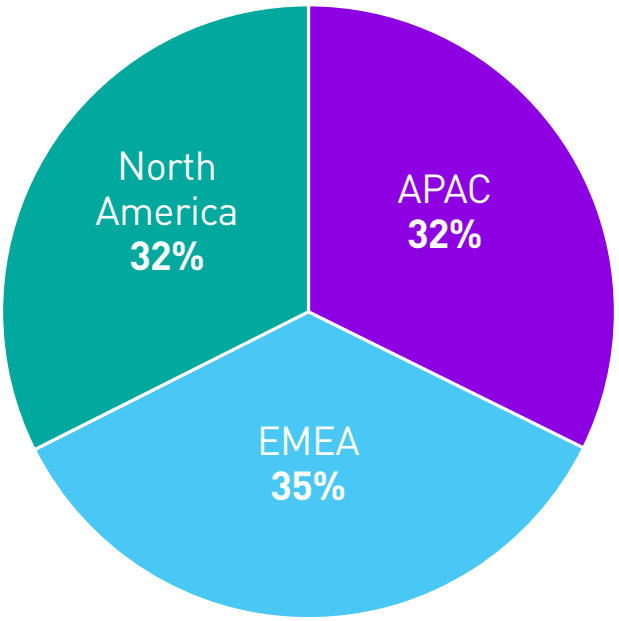
- **Geography:** North America, APAC, and EMEA each make up about one-third of respondents.
- **Industry:** Financial services, technology, and retail and consumer goods each make up about one-fifth of respondents, with remaining respondents working in a range of other industries. Of note, we estimate that at least 20% of our total retail and consumer goods respondents work in businesses specializing in online retailing, with the remainder relying on online channels as just part of an overall sales strategy.
- **Role:** Lawyers (in-house and outside counsel) account for roughly one-quarter of respondents, and executives (C-suite, vice president, and director level) comprise the rest.

Throughout, we provide context and quotations from leading executives and attorneys dealing with AI issues, both in-house and as outside counsel, and from BRG experts.

Which best defines your position?



Regional breakdown



Contributors

Richard Allen

Local Principal, Dispute Resolution and International Arbitration Practice Groups

Baker McKenzie
Singapore

Ben Allgrove

Chief Innovation Officer and Partner, IP, Data, and Technology Team

Baker McKenzie
London

Elizabeth Chan

Registered Foreign Lawyer

Stevenson, Wong & Co.
Hong Kong

Steve Fraley

Former Global Data Protection Officer

Vonage
Los Angeles

John Groom

Partner, IP and Technology Team

Baker McKenzie
London

Yuankai Lin

Partner specializing in commercial and technology disputes

RPC Premier Law
Singapore

Byron Phillips

Partner and disputes lawyer, Litigation, Arbitration, and Employment Practice

Hogan Lovells
Hong Kong

Adam Rouse

Senior Counsel and Director of e-Discovery Operations

Walgreens
Chicago

BRG Contributors

Shawn Ashworth

Managing Director | Washington, DC

Shawn Ashworth co-leads BRG's Retail Performance Improvement practice and focuses on implementing operational improvements to drive financial results. He is a retail and consumer products industry expert with more than twenty years of consulting experience. He has delivered performance improvement projects for dozens of clients across specialty, department stores, and wholesale brands.

Michael Canale

Managing Director | New York

Michael Canale is a leader in BRG's Financial Institution Advisory practice where he works with top-fifty financial institutions, cryptocurrency exchanges, private equity firms, and nonbank servicers. He works on matters across operations, risk and compliance, data analytics, blockchain, and process automation. He has experience leading financial crime audits, risk assessments, enforcement action remediation, acquisition due diligence, organizational design, technology development, and implementation of advanced tools including data visualization, workflow, machine learning, and AI.

Richard Finkelman

Managing Director | Washington, DC

Richard Finkelman is a nationally recognized technology expert who brings more than thirty years of experience helping clients manage information and technology in litigation, compliance, and business matters. He is a frequent speaker at industry events and was named a 2024 AI Visionary by Relativity.

Murali Gokki

Managing Director | Atlanta

Murali Gokki co-leads BRG's Retail Performance Improvement practice. He brings more than twenty years of experience delivering high-impact strategic and business transformational solutions for global retail, wholesale, and consumer products companies. He has served as a trusted advisor to private equity firms, C-suite leaders, and boards on addressing strategic and operational challenges and has led projects in North America, Europe, and Asia.

Erick Gunawan

Managing Director | Singapore & Sydney

Erick Gunawan is head of BRG's Cyber Forensics and eDiscovery practice in APAC. He has over twenty years of experience in computer forensics, compliance investigations, crypto-tracing and investigations, dawn-raid readiness, and eDiscovery and has expertise in enhanced document-review technology using AI models and machine learning.

David Parker

Managing Director | London

David Parker advises companies facing competition investigations in relation to agreements, abuses of dominance, market studies, and investigations and mergers across national and supranational jurisdictions. He acts as an economic expert in litigation cases, including standalone cases relating to breaches of competition law and follow-on damages cases arising from breaches of competition and other laws.

Cleve B. Tyler

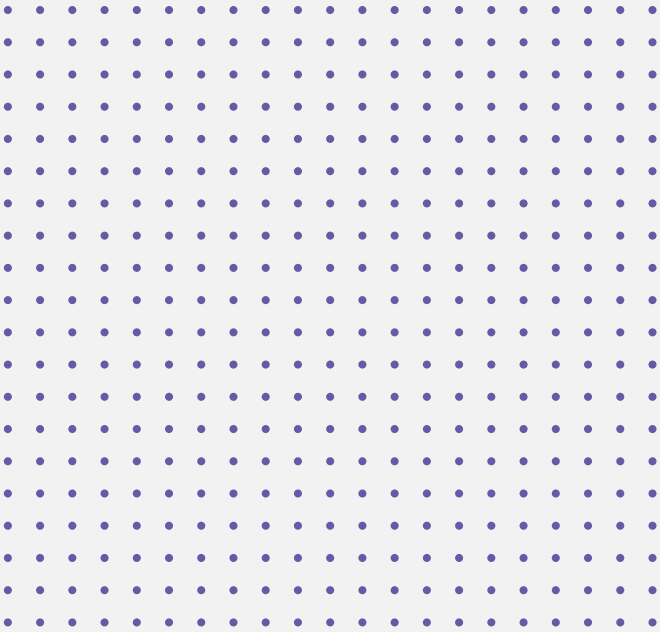
Managing Director | Washington, DC

Cleve B. Tyler, PhD, is a managing director at BRG who specializes in applying economic analyses to antitrust, intellectual property, and damages issues. An economic consultant with more than twenty-five years of experience, he also teaches, writes, and speaks about competition and intellectual property topics. He has testified at deposition and trial in federal court, in state court, in regulatory proceedings and at arbitration.

Amy Worley

Managing Director & Associate General Counsel | Washington, DC

Amy Worley is an expert in the fields of global data privacy and data protection regulation, data governance, and data ethics, including the growing field of AI regulation. She serves as a fractional data protection officer for organizations worldwide, providing gap and risk assessments, developing remediation plans, liaising with global regulatory bodies, assisting clients in responding to security incidents, and advising boards of directors on data compliance related risk.



About BRG

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: economics, disputes, and investigations; corporate finance; and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working across borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next.

THINKBRG.COM