BRG

INTELLIGENCE THAT WORKS

AI INDUSTRY SPOTLIGHT SERIES

AI in Financial Institutions: Staying Ahead in the AI "Arms Race"

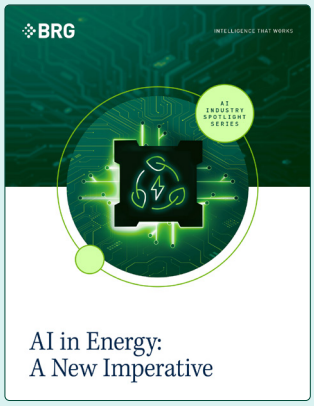
AI Industry Spotlight Series

This report—the third installment in BRG's *AI Industry Spotlight Series*—examines how financial institutions are adopting artificial intelligence (AI) amid margin pressures, operational complexity, and evolving regulatory expectations.

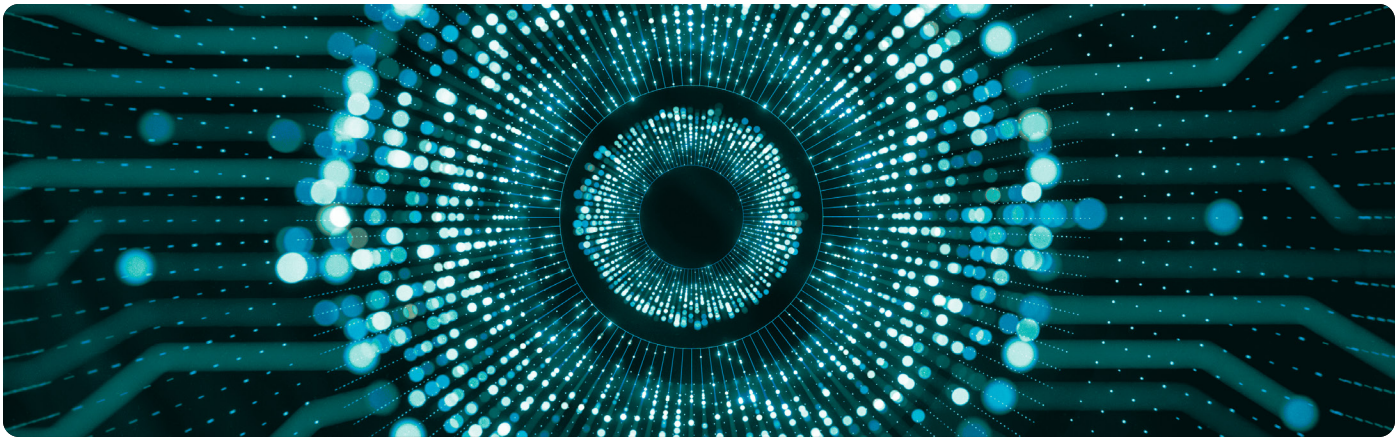
The series launched in November 2025 and has examined AI's influence on the retail and energy sectors. It is part of a broader BRG research initiative exploring AI implementation, impact, and risk across key industries, continuing BRG's effort to deliver timely insights to help organizations unlock the value of AI.

Read the first two reports in the series:

AI in Retail: In Pursuit of Meaningful AI Adoption



AI in Energy: A New Imperative



Financial institutions have been early adopters of artificial intelligence (AI). But a new survey of industry leaders suggests that auditable returns, institution-wide adoption, and comprehensive regulatory frameworks remain elusive.

Financial institutions have been early adopters of AI. But a new survey of industry leaders suggests that auditable returns, institution-wide adoption, and comprehensive regulatory frameworks remain elusive.

Financial institutions around the world are integrating AI tools rapidly—and for good reason. Efficiency gains in areas like cybersecurity, fraud detection, and corporate functions have delivered significant wins. For instance, AI initiatives saved JPMorgan Chase $1.5 billion in fraud prevention, trading, and operational improvements.

In today's fast-evolving business landscape, maintaining the status quo may not be enough, particularly for smaller players without deep pockets for AI investment. On one hand, bad actors are moving as fast as—or faster than—good ones, creating something of an "AI arms race."

"Financial institutions are in constant combat," says Samantha Welch, a managing director at BRG. "As AI tools become more advanced, they also become more universally used, which means a sophisticated fraud scheme is much easier to perpetrate with limited resources."

On the other hand, uneven adoption and operational challenges may contribute to a slump in true innovation. "I see so many headlines like 'We can do more with less now,' but what about doing things we never thought possible?" asks BRG Managing Director Michael Canale. "We need to think more about the opportunities to harness AI to do new and exciting things and less about how to replace people and processes."

Regulators are signaling they want to see banks use AI tools to do more than just cut costs. Recent proposed rulemaking from the Financial Crimes Enforcement Network indicates that when determining whether to take enforcement action against a bank, consideration could be given to the bank's employment of AI tools to provide useful information to law enforcement and national security officials. Regulators also remain acutely aware of systemic risks posed by AI, particularly around cybersecurity, as evidenced by the Department of the Treasury's April meeting of Global Systemically Important Banks.

Similar to recent headlines, BRG's survey found that fraud and financial crime risks and competitive pressures are primary areas of focus for financial institutions. Meanwhile, workforce and reputational risks appear to be underappreciated, as only half of respondents consider their organizations fully equipped to manage AI-related risk.

These are some of the top takeaways from BRG's survey of 110 executives leading AI implementation efforts at their respective financial institutions, including banks, nonbank institutions, and financial technology companies across the globe.

Below, we discuss five key takeaways.

Key Findings

1. Almost all respondents expect AI adoption to increase in 2026, citing significant efficiency gains in customer service, corporate functions, and cybersecurity.
2. More than six in ten organizations have implemented AI in cybersecurity, fraud detection, and corporate functions—though adoption lags in other key areas.
3. Fraud and financial crime, credit risk, and regulatory enforcement are expected to see the greatest increase in AI-related risk exposure, even as organizations appear to underestimate reputational and workforce vulnerabilities.
4. Only half of respondents believe their AI policies are fully equipped to manage risk in a changing regulatory environment, with concerning gaps in data security/ management and workforce impact.
5. Most organizations measure return on investment from AI-enabled initiatives via financial and operational metrics.

Examples of AI Use Cases Across Financial Institutions Functions

Collections and recovery: early delinquency detection, repayment predictions, automated outreach

Compliance and regulatory monitoring (excluding Bank Secrecy Act (BSA)/anti-money laundering (AML)): policy breach detection, automated compliance testing, transaction testing, documentation, customer complaints

Corporate functions: contract analysis, finance automation, Human Resources analytics, marketing

Credit decisioning and bifurcation: application triage, risk segmentation, routing, preapproval decisions

Customer service and personalization: chatbots, onboarding, personalized guidance

Cybersecurity and information security: threat intelligence, vulnerability detection, incident response

Data management and modeling: data quality monitoring, model deployment

Financial crime screening and transaction monitoring: BSA/AML, sanctions monitoring

Fraud detection: identity fraud, claims fraud, transactions fraud, trade surveillance

Loan servicing: payment processing, account maintenance, servicing workflows

Underwriting and pricing: credit scoring, verification, risk assessment, pricing decisions

1. Almost all respondents (94%) expect AI adoption to increase in 2026, citing significant efficiency gains in customer service, corporate functions, and cybersecurity.

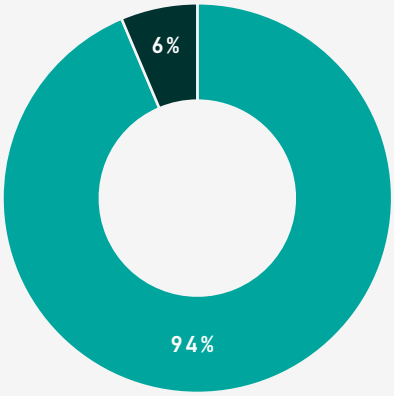
AI use in financial institutions continues to accelerate. Nearly all respondents (94%) report that they expect AI adoption to increase in 2026, with 6%—likely aggressive early adopters—anticipating it will remain the same. None expect a decrease. This is significant, as over half of respondents (54%) report actively using AI in most core functions, and 42% use it in several.

"Ninety-four percent of executives expect adoption to grow in 2026," said Peter Smith, a managing director and head of BRG's AI and Decision Intelligence practice. "That figure reflects commitment more than maturity, but it's a clear sign that organizations are seeing enough value from early investment to keep leaning in, even amid regulatory and operational complexity."

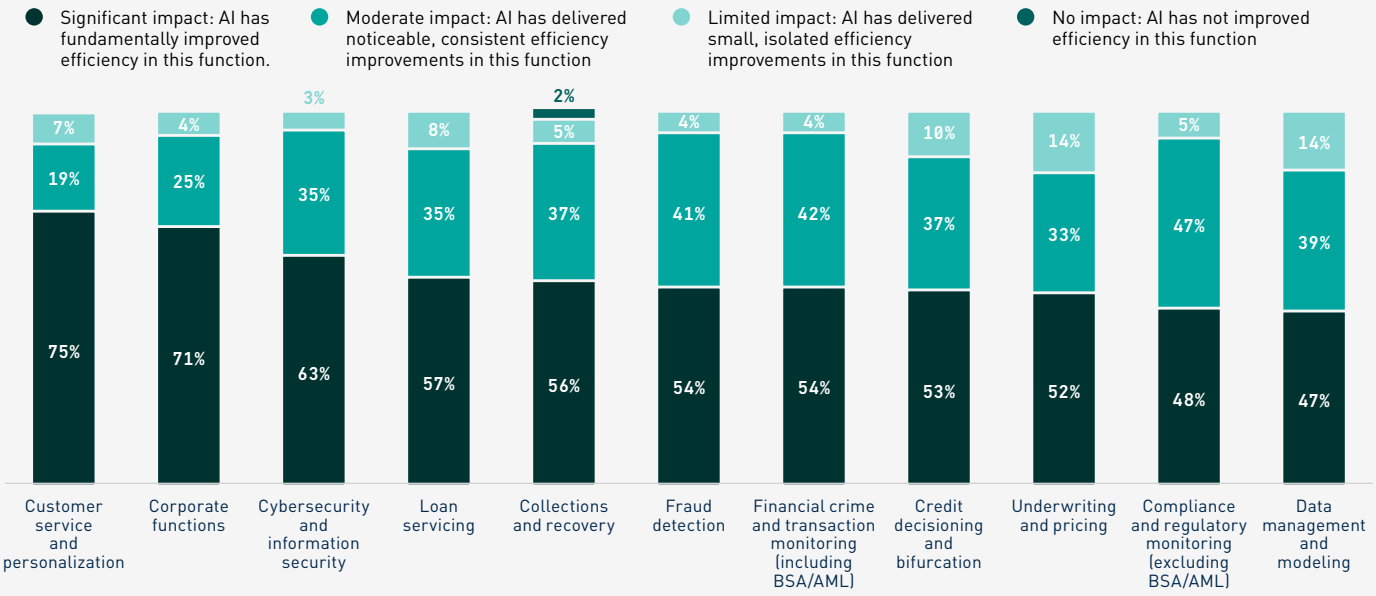
Reported efficiency gains support executives' stated enthusiasm. The overwhelming majority of respondents who have already implemented AI in the surveyed functions said that AI has fundamentally improved efficiency for customer service and personalization (75%), corporate functions (71%), and cybersecurity and information security (63%). Over half said the same about key areas like fraud detection and financial crime.

"In customer service and corporate functions, organizations can see tangible improvements, be it streamlined processes or reduced staff," said Paul Noring, a BRG managing director and a leader of the firm's Financial Institution Advisory practice. "Fraud and financial crime detection, however, remain challenging despite widespread AI adoption, largely because of the 'arms race' quality wherein heightened and more sophisticated use by bad actors fuels heightened spend and preventive actions by financial institutions."

Expected Change in AI Adoption



AI's Impact on Efficiency



2. More than six in ten organizations have implemented AI in cybersecurity, fraud detection, and corporate functions—though adoption lags in other key areas.

We asked respondents about their organizations' AI implementation across eleven key areas. One important takeaway: Adoption remains highest in the lowest-risk areas with tangible return on investment (ROI) (e.g., customer service—like one company that cut 45% of its customer support workers to replace them with AI); and in areas where the need to stay ahead of industry trends, such as identifying or deterring bad actors, is most prominent.

Case in point: More than six in ten have implemented AI in cybersecurity (65%), fraud detection (64%), and corporate functions (62%). Over half have implemented AI in compliance and regulatory monitoring (55%), customer service (54%), and data management (54%)—though there may be ample opportunity left on the table, especially when it comes to compliance and regulatory monitoring.

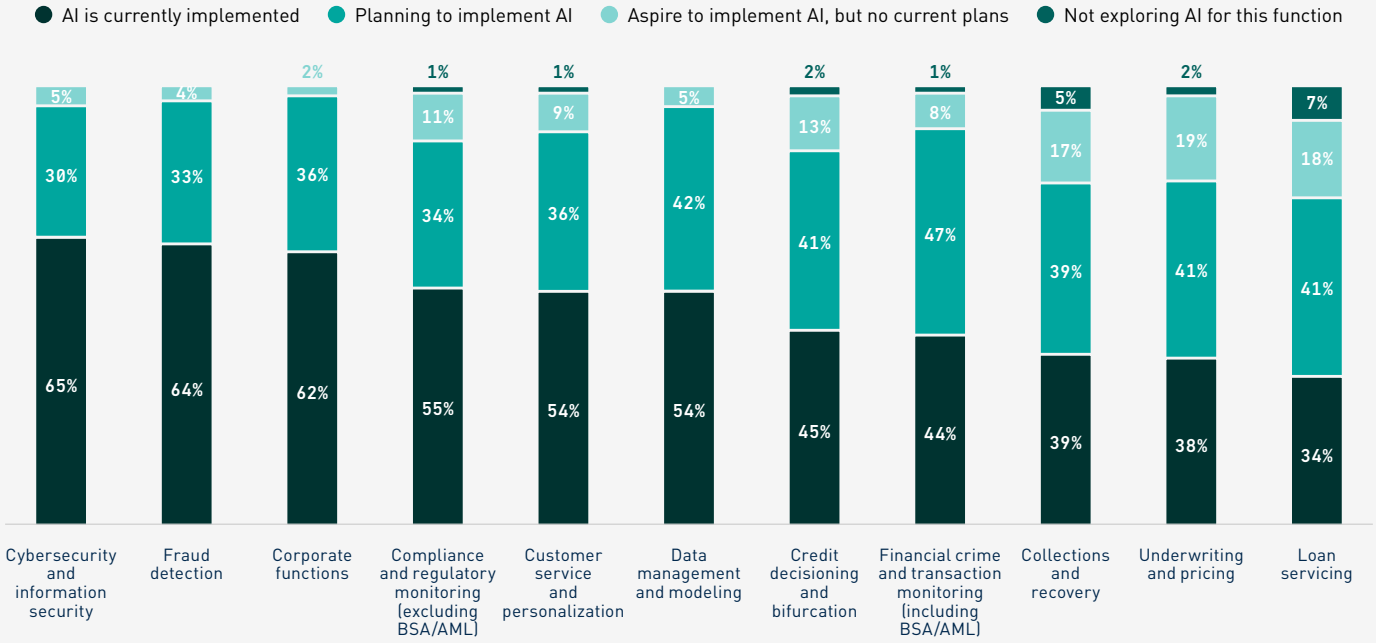
"For years, the compliance industry has been searching for the silver bullet to automate things like risk assessments, testing, and policy updates, but data quality issues, legacy systems, budget limitations, and technological roadblocks have made it a challenge," says Mr. Canale. "Tools like optical character recognition (pulling data from documents), natural language processing (analyzing voice and text), advanced data analytics, and robotic process automation were part of the first wave of innovation. AI takes it to the next level, incorporating many concepts with models that can evaluate inputs and outputs, compiling analyses into a comprehensive package."

There may be other untapped opportunities. For instance, nearly 10% of respondents said they have no current plans to implement AI in financial crime and transaction monitoring. Even more said the same about loan servicing (25%), collections and recovery (22%), and underwriting and pricing (21%)—even as these areas led to significant efficiency gains for more than half of those surveyed.

What are your most effective AI use cases?

CYBERSECURITY
"We implemented AI to detect real-time cybersecurity threats."
"Anomaly detection identifying network threats in real time."
FRAUD DETECTION
"We developed a fraud monitoring tool that can better identify fraudulent transactions."
"AI-based fraud detection to flag suspicious transactions faster and reduce false positives."
CORPORATE FUNCTIONS
"Natural language processing tool analyses social media sentiment, alerting teams to brand reputation risks."
"Sentiment analysis prioritizing high-risk customer support tickets."

Implementation Status



3. Fraud and financial crime, credit risk, and regulatory enforcement are expected to see the greatest increase in AI-related risk exposure, even as organizations appear to underestimate reputational and workforce vulnerabilities.

In terms of the greatest increase and foremost concerns in risk exposure over the next three years, respondents cited core banking vulnerabilities including fraud and financial crime (49%), credit risk and underwriting models (42%), and regulatory and enforcement risk (42%). Respondents specifically highlighted "AI-enabled fraud outpacing detection and controls," "[underwriting] model drift," and "AI-related investigations and AI washing."

Ms. Welch agrees that fraud and financial crime is the top threat to financial institutions, along with cybersecurity. As AI proliferates, financial institutions will be "concurrently managing risks related to identity management across the entire ecosystem, including fraudulent identification in onboarding processes, impersonation of financial institution personnel within internal access management protocols, and external actors posing as legitimate representatives to defraud customers or other third parties or spread misinformation to create market impacts."

Simultaneously, institutions face a rapidly evolving regulatory landscape. Growing US state data privacy laws, such as in Colorado and California, alongside frameworks like the European Union (EU) AI Act are raising expectations around transparency and governance.

"Financial institutions are already heavily regulated and face constant litigation risks, and AI just raises the bar," said Michael Hollerich, a BRG managing director. "It's not enough for models to produce outputs; when using AI, firms need governance, documentation, testing, and explainability sufficient to defend those outputs, particularly in higher-risk areas such as credit, fraud, and customer-facing decisions. The use of AI must be governed by an enhanced enterprise risk program, not just a single control."

Institutions also may be underestimating broader risks. For instance, only 18% of respondents cite reputational risk—from AI-driven decisions or failures—and 14% cite workforce and labor considerations as areas where risk exposure is expected to increase significantly over the next three years. The latter issue, in particular, may be underestimated, as recent examples—including a fintech company laying off nearly half its workforce and at least one global financial institution reportedly considering a 10% reduction as banks shift work to AI—highlight the potential scale of disruption. These may only be early indicators of a broader shift; traditional players should take note.

"This industry was caught back-footed with the emergence of digital-first banks, and AI-first banks will emerge to threaten their market standing," said Jen Langusch, a managing director in BRG's AI practice.

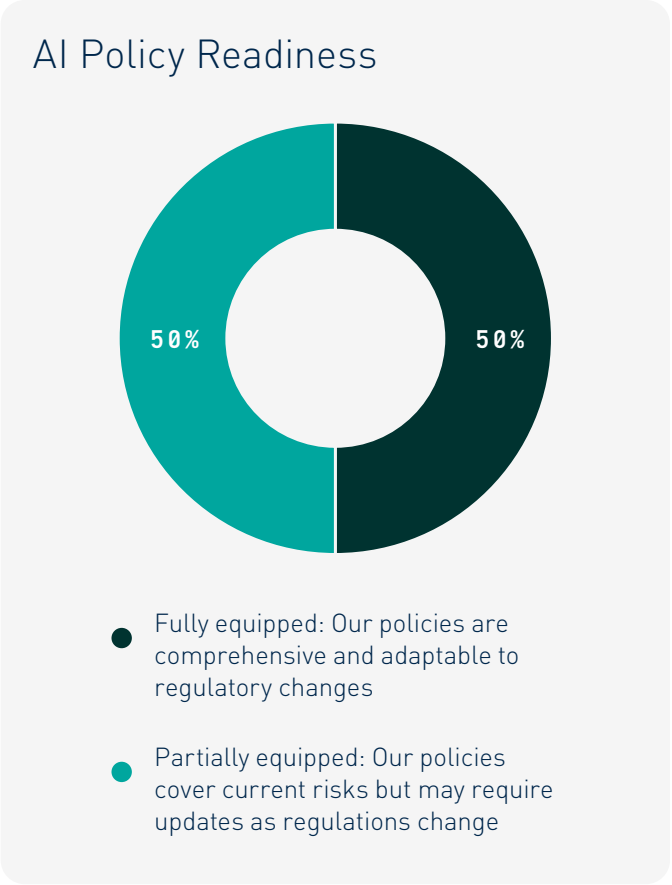
Areas Where Greatest Increases in AI-Related Risk Is Expected *(next three years)*

4. Only half of respondents believe their AI policies are fully equipped to manage risk in a changing regulatory environment, with concerning gaps in data security/management and workforce impact.

Financial institutions already operate within complex supervisory frameworks spanning data privacy, model governance, consumer protection, information security, and third-party oversight. Cross-border institutions must also navigate an evolving patchwork of jurisdiction-specific AI and privacy requirements.

Yet only half of respondents considered their organizations fully equipped to manage risk in a changing regulatory environment. This could be less a reflection of internal capability than of ongoing uncertainty around how these technologies will ultimately be governed. Organizations may feel unready to manage risk simply because they do not yet know what those risks will be.

"Financial institutions should expect significant regulatory evolution around AI, from strict model governance expectations to new laws like the EU AI Act," says Amy Worley, leader of BRG's Global Information Compliance Advisory practice and author of *The Confidence Advantage: Optimizing Privacy, Cybersecurity and AI Governance for Growth*. "As regulations change rapidly and extensively, staying aware and reactive is necessary. We recommend financial institutions implement principle-based governance frameworks designed to meet existing compliance requirements but flexible enough to meet the moment in a dynamic regulatory environment."



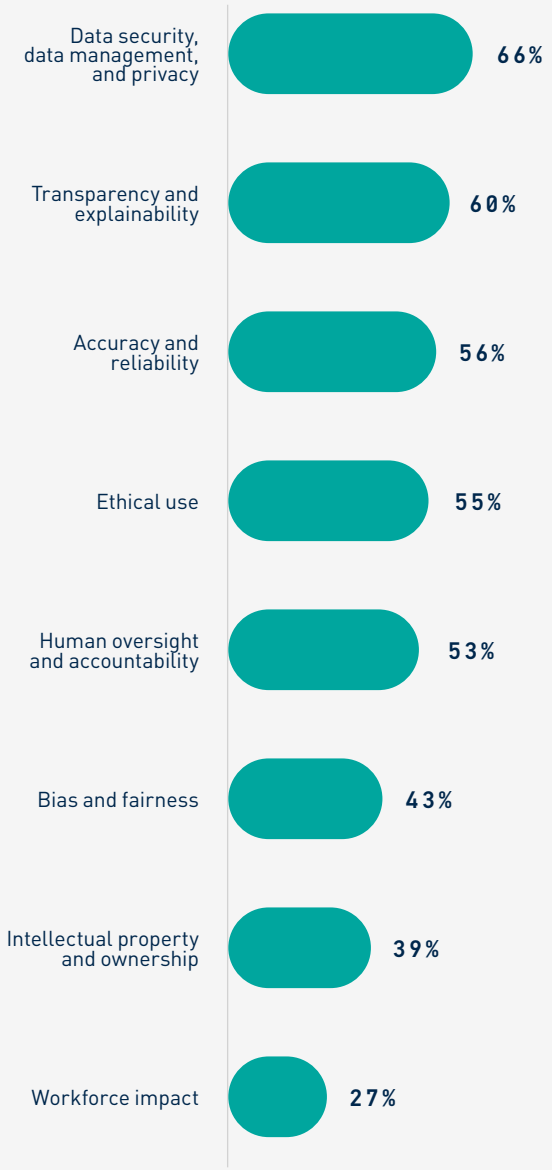
Policies concentrated largely on data security, data management, and privacy (66%), and transparency and explainability (60%). Given that AI models rely heavily on customer data, including demographic information, product usage, and transaction records, any security gap is significant.

"There are ample opportunities to improve operational readiness," says Mr. Canale. "The biggest gaps are in establishing enterprise-wide AI governance frameworks, implementing policies on AI usage (what is authorized and what is not) and data privacy, model validation of AI and machine learning models, and the need for periodic training."

Another notable blind spot is workforce impact, which only 27% of policies address. Respondents' apparent lack of concern about workforce and labor risk suggests that organizations may not be adequately considering how AI adoption could affect employees. Without careful planning, these workforce impacts could also create reputational risks.

"Leaders in financial services are laser-focused on fraud and compliance, but they're missing the real landmine: brand reputation. The industry is littered with examples of firms that won the efficiency argument and lost the trust war, from Goldman Sachs' Apple Card bias scandal to Klarna's public AI reversal," says Mr. Smith. "What makes this uniquely dangerous today is surface area. Every new AI touchpoint, chatbot interaction, and automated credit decision is a moment where a customer, investor, or regulator forms an opinion of your brand. The more you deploy AI, the more exposure you have."

Areas of Risk Addressed by AI Policy



5. Most organizations measure ROI from AI-enabled initiatives via financial and operational metrics.

With AI spending in financial services projected to reach over $125 billion in 2028, organizations are under mounting pressure to show ROI to stakeholders. But few are likely to acknowledge when those returns fall short, and many are still developing reliable ways to measure them.

Fortunately, financial institutions are taking active steps in this arena. When asked how ROI from AI-enabled initiatives is evaluated in their organizations today, respondents reported using quantitative financial metrics (45%), operational metrics (35%), usage or adoption metrics (15%), and qualitative or anecdotal assessment (4%).

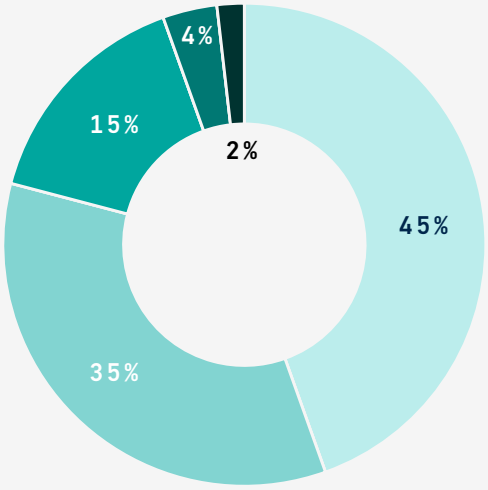
AI often requires meaningful capital, integration, governance, and operating investment. Every company would be best served measuring against well-structured key performance indicator (KPI) targets rather than implementing new tools without clear objectives. Those using metrics based on adoption, for instance, should potentially reconsider their approach.

"Correlating high AI adoption with success is like awarding Olympic medals for hours trained versus actual performance," said Ms. Langusch. "Organizations need to move beyond surface-level adoption metrics and instead track AI's impact broadly, including what drives revenue growth, operational efficiency, and risk-adjusted returns."

Rigorous AI ROI measurement requires more than one metric. A credible ROI framework should assess multiple dimensions of value from both the balance sheet and income statement to determine whether AI initiatives deliver measurable impacts after any offset from added risk management routines that the institution must consider is accounted for. Industry leaders must establish clear baseline measurements before AI deployment and track several dimensions of impact. However, attribution grows challenging as AI becomes embedded across myriad processes, and it can be harder to isolate direct cause and effect.

Organizations that assess top-line growth and expansion as a key metric tend to outpace those that focus purely on productivity and efficiency. Thus, any ROI tracking should include deliberate inclusion of growth metrics, even if that boils down to quality improvements.

Evolution of ROI from AI Initiatives



Align AI with business strategy and measurable value.

Strengthen data strategy and infrastructure.

Define KPIs and track performance.

Establish enterprise-wide governance and risk management.

Build capabilities and embed AI into operations.

Best Practices for Financial Institutions Adopting AI

Best Practices for Financial Institutions Adopting AI

Our findings and industry experience suggest a gap between ambition and execution in AI adoption across financial institutions. Many organizations recognize AI's potential, legacy systems, regulatory complexity, and fragmented data, but environments often limit impact. Without a clear strategy and governance, AI initiatives risk remaining siloed experiments rather than delivering enterprise-wide value.

To maximize the potential of AI, financial institutions should consider the following best practices:

1. Align AI with business strategy and measurable value.

Institutions should prioritize AI initiatives that address specific business challenges, such as fraud reduction, cost efficiency, and revenue growth, rather than pursue technology for its own sake. It is critical to have a clear roadmap with defined use cases and expected ROI that balances quick wins that demonstrate early value with longer-term investments in enterprise AI capabilities. Sustainable growth comes from institutionalizing AI, not just one-off projects.

2. Strengthen data strategy and infrastructure.

Effective AI depends on high-quality, well-governed, and accessible data. Financial institutions should invest in improving data quality, data attribution methods, and governance frameworks while ensuring compliance with evolving data privacy requirements.

3. Define KPIs and track performance.

Organizations should establish clear metrics at the outset of each AI initiative to measure financial, operational, and customer impact. Tracking performance against defined KPIs helps validate outcomes, guide investment decisions, and ensure alignment with both business objectives and risk appetite.

4. Build capabilities and embed AI into operations.

Successful AI adoption requires investment in skills, clear ownership, and strong cross-functional collaboration. Institutions should embed AI into core workflows, manage organizational change, and continuously refine models and use cases to scale impact over time.

5. Establish enterprise-wide governance and risk management.

Strong governance is essential to scale AI responsibly. Institutions should implement clear policies on acceptable AI use, establish cross-functional oversight, and integrate AI into existing model risk management frameworks. Many AI applications should be viewed through the same lens as end-user computing and model risk management: they require inventory, governance, and independent validation to ensure they are understood and controlled.

Financial institutions should ensure employees are trained in what to look for when handling customer accounts and activity; and consider how employees themselves could be manipulated.

"It's important that training does not end with employees," says Ms. Welch. "Financial institutions should also consider educating customers on how to protect themselves."

Methodology

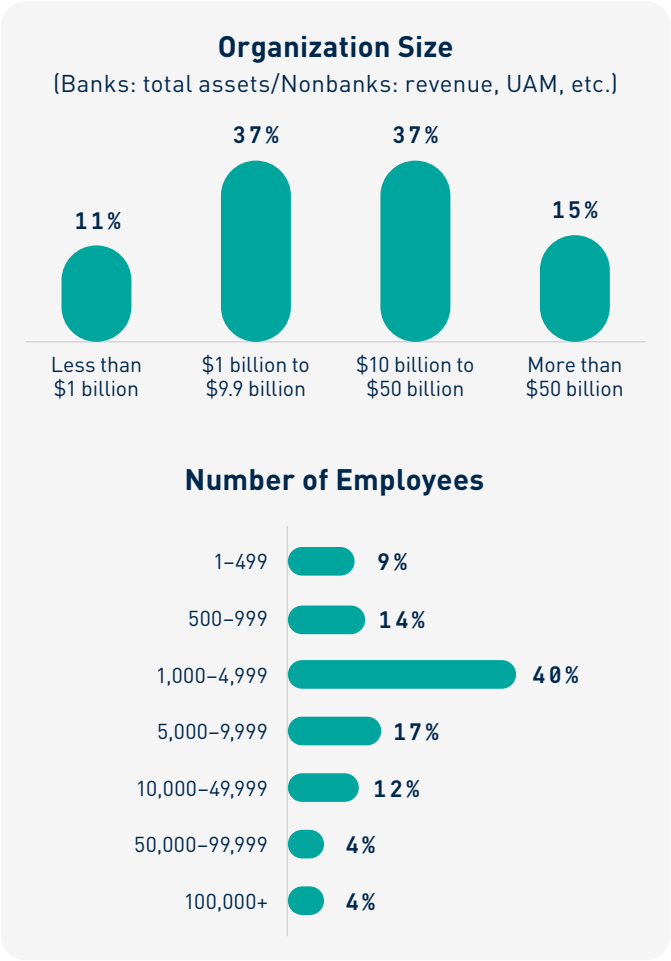
The research for this report was conducted in January 2026 via a quantitative survey of 110 executives and leaders in the financial institutions sector, covering traditional banking (sixty respondents), nonbank financial institutions (twenty respondents), and financial technology companies (thirty respondents).

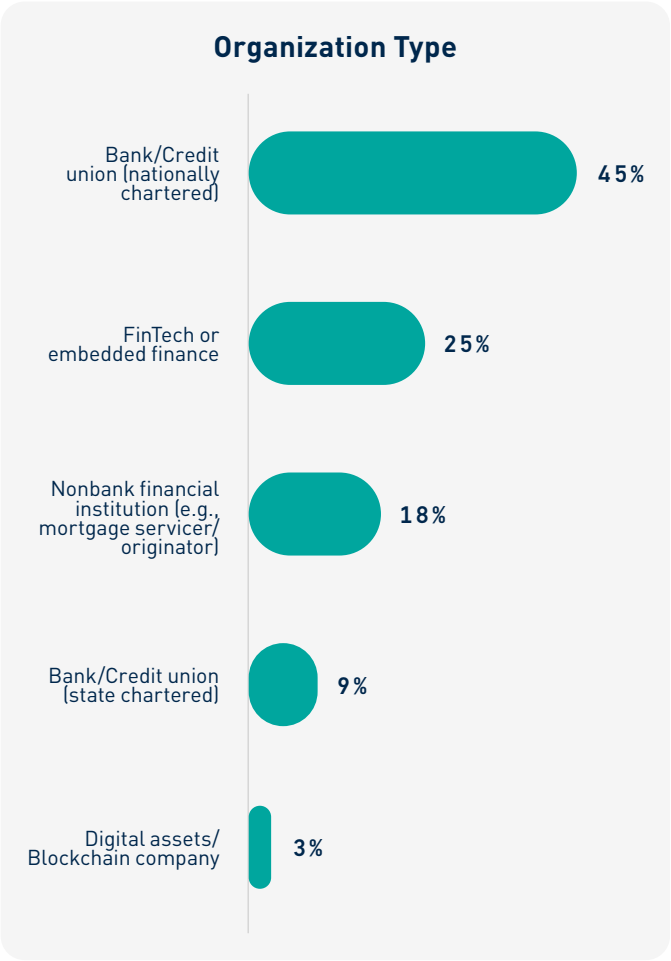
The respondent base was global, with operations across Asia-Pacific, Europe, the Middle East and Africa, Latin America, and North America.

Respondents held leadership positions at their organizations and were involved in their organization's AI implementation efforts.

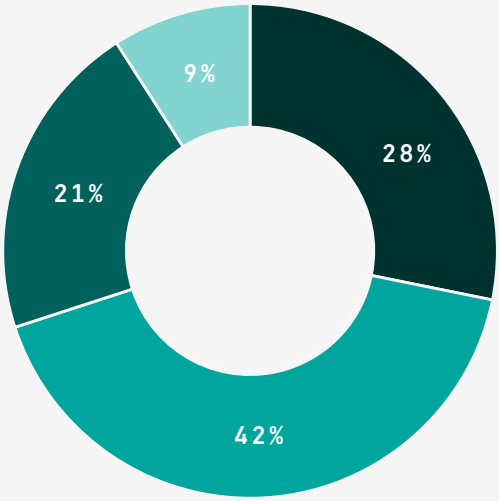
This is the third report in BRG's *AI Industry Spotlight Series* that tracks AI's influence across key industries. The first two editions explored AI in retail and AI in energy.

Due to rounding and questions asking for more than one response selection, data may not add up to 100%.



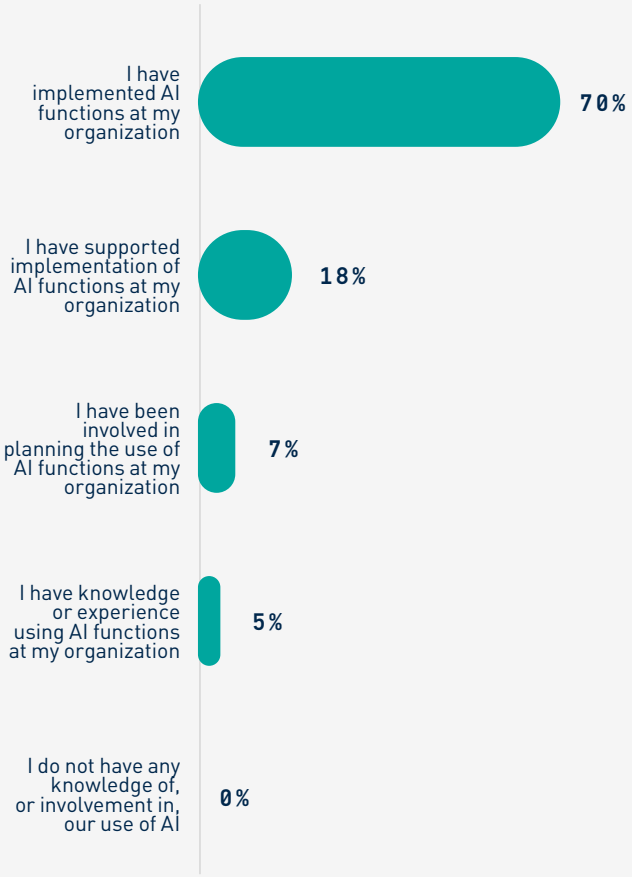


Position



- CEO/President/Chair
- C-suite other than CEO (e.g., CFO, CIO, CMO, COO, CRO)
- Senior leadership other than C-suite: Executive VP, VP, Managing Director, or other senior-level title
- Business-line leader (e.g., head of Retail Banking, Commercial Banking, Investment Banking)

Experience with AI



FOR EXPERT GUIDANCE AND TAILORED STRATEGIES TO ENSURE SUCCESSFUL AI ADOPTION, CONTACT BRG'S FINANCIAL INSTITUTION ADVISORY PRACTICE.

Paul Noring
Managing Director
pnoring@thinkbrg.com
202.839.3925

Michael Canale
Managing Director
michael.canale@thinkbrg.com
631.662.7931

John DelPonti
Managing Director
jdelponti@thinkbrg.com
704.877.0441

Michael Hollerich
Managing Director
mhollerich@thinkbrg.com
847.721.4890

Vincent Urbancic
Managing Director
vurbancic@thinkbrg.com
202.480.2752

Samantha Welch
Managing Director
swelch@thinkbrg.com
646.589.0575

BRG combines world-leading academic credentials with world-tested business expertise, purpose-built for agility and connectivity, which sets us apart—and gets you ahead.

Our top-tier professionals include specialist consultants, industry experts, renowned academics, and leading-edge data scientists. Together, they bring a diversity of proven real-world experience to economics, disputes, and investigations; corporate finance; and performance improvement services that address the most complex challenges for organizations across the globe.

Our unique structure nurtures the interdisciplinary relationships that give us the edge, laying the groundwork for more informed insights and more original, incisive thinking from diverse perspectives that, when paired with our global reach and resources, make us uniquely capable to address our clients' challenges.

VISIT THINKBRG.COM TO LEARN MORE.