ECONOMIST IMPACT

Intelligent banking: The future ahead

Supported by SAS

Contents

Foreword by SAS

Disruption. Transformation. Evolution. These are just a few of the words frequently used to describe the global banking industry—and for good reason. The past two decades have brought sweeping change, and the post-pandemic years have accelerated the pace of transformation to warp speed.

Banks have long weathered macroeconomic shifts, wars, political transitions, rising financial crime and a complex global regulatory landscape. But today, these forces are hitting harder and faster, creating volatility not seen in decades.

Challenges abound from ongoing digitalisation; competition from fintechs and non-banks; digital currencies and open banking; and perhaps the most profound innovation and disruption of the intelligent age: AI.

Each of these influences leads down its own proverbial rabbit hole—a complex maze of interconnected paths, sidetracks and hidden pitfalls. With so many diverse and fast-moving forces at play, how can banks chart a clear, manageable course? Where should they focus, and how should they prioritise when everything demands immediate attention, well-defined yet flexible strategies, enabling technologies, excellent execution and a skilled workforce?

How can banks protect their current operations while innovating for the bank of tomorrow?

To answer these questions, Economist Impact surveyed 1,700 senior banking executives to identify the most pressing trends and challenges facing global banking over the next decade, and to understand how those priorities are shaping the now and the next. While outliers and surprises will always exist, the results of this study reveal broad alignment. Banks recognise the shifts that demand their focus and are strengthening foundational frameworks, evolving existing infrastructure, adopting and innovating with new technologies, upskilling talent, and tapping into the agility of strong vendor and partner ecosystems.

Stability, resilience and transparency are critical, because at the centre of everything lies the customer relationship—the most fragile and powerful influence of all. That relationship can only be sustained and grown through a clear demonstration of customer centricity underpinned by a strong foundation of trust.

Julie Muckleroy
Global Banking Strategic Advisor
SAS

About the research

Intelligent banking: The future ahead, an Economist Impact report supported by SAS Institute, examines the forces poised to reshape the industry over the next decade and the strategies banks are adopting to remain competitive. It builds on insights from *Banking in 2035*, published in 2023. The first publication outlined three possible scenarios for the industry, whereas this report focuses on one: intelligence-driven digital innovation. It offers tangible guidance to financial institutions as they navigate disruptive forces and pursue sustainable growth.

The findings presented here are based on a comprehensive research programme comprising a literature review, an executive survey and in-depth interviews. The survey gathered insights from 1,700 senior executives (VP-level and above) across three segments: commercial/corporate banking, retail banking and financial technology/digital banking. At least 30% of respondents work in each segment. The banks we surveyed are located in North America (the US and Canada), Latin America (Brazil), Asia Pacific (Australia, Japan, India and Singapore), Europe (France, Denmark, Germany, Ireland, Italy, the Netherlands, Spain, Sweden and the UK), Africa (South Africa), and the Middle East (the United Arab Emirates and Turkey). They have annual revenues of at least US$10m, with about 50% generating revenues of more than US$500m.

To provide deeper insights into the challenges and opportunities facing financial institutions, we conducted an interview programme with industry professionals that complements the survey. We extend our gratitude to the following individuals (listed alphabetically by last name) for their valuable time and contributions:

- **Zechariah Akinpelu**, chief information security officer, Unity Bank
- **Piotr Gonera**, director of global corporate and investment banking, Mizuho Bank
- **Tobias Klingel**, head of information security, Aspire
- **Roisin Levine**, head of UK and Europe bank partnerships, Wise Platform, Wise
- **Nimish Panchmatia**, chief data and transformation officer, DBS Bank
- **Jas Shintré**, executive director - head of technology, Standard Chartered Bank
- **Thomas Wallace**, chief risk officer, Revolut UK
- Two senior executives from banks with more than US$50bn in annual revenue (on background)

The research was managed by the following Economist Impact project team:

- **John Ferguson**, project advisor
- **Melanie Noronha**, project director
- **Ashish Niraula**, project manager
- **Jeremy Gantz**, writer

Executive summary

The global banking sector is in the midst of profound change: technology is advancing rapidly, while geopolitical tensions and economic uncertainty reshape financial systems. Strains between the East and West have fractured global financial flows and are driving regulatory divergence. Sharp changes in interest rates have increased credit and liquidity risks, threatening wider financial instability.

As artificial intelligence (AI), blockchain and other emerging technologies transform how institutions operate, banks are finding themselves both empowered and exposed. These technologies help banks respond to macroeconomic and geopolitical shifts, but also introduce challenges, from fraud to ethical concerns over AI deployment. To manage these risks, banks must strengthen data security, management and governance. As technology intensifies competition and regulation becomes more complex, banks must balance innovation with compliance and customer trust.

How can banks prepare for this new era of banking? Drawing on a global survey of 1,700 senior banking executives, Economist Impact examines their strategic priorities as they build future-ready foundations for their organisations. The insights in this report equip banks with the strategies needed to thrive in this rapidly evolving environment, focusing on responsible AI deployment, data management, fraud prevention, risk assessment, customer relationships and innovation.

Key findings of the research

- **Experimentation with generative AI (genAI) is rife, but returns are scarce.** Nearly all banks surveyed report genAI implementation in some form, but more than half are seeing limited returns, with some even reporting no returns. Prioritising revenue-generating and cost-saving applications can help drive returns. In 2025, banks will work to scale successful genAI initiatives while also reassessing its suitability for others.

- **AI increases the threat of fraud, but is also a tool for prevention.** AI-generated deepfakes and synthetic identities are banks' biggest fraud challenges, but AI-powered detection is also considered the most effective countermeasure. Using AI responsibly—by reducing model bias, ensuring ethical data use and explaining its decisions—can make it a more effective tool for fraud prevention.

- **A strong governance framework can enhance data security and enable responsible adoption of technologies as they evolve.** These frameworks must clearly define data ownership and accountability in order to be effective. Crucially, AI frameworks can serve as blueprints for integrating future innovations, including quantum computing.

- **Despite rising compliance costs, most banks see new regulations—especially on AI, blockchain and open banking—as enablers of innovation rather than obstacles.** These rules provide common standards and guardrails, helping firms accelerate the integration of advanced technologies. Rising geopolitical tensions are likely to lead to regulatory divergence on data privacy and sovereignty, requiring banks to navigate a patchwork of laws across markets.

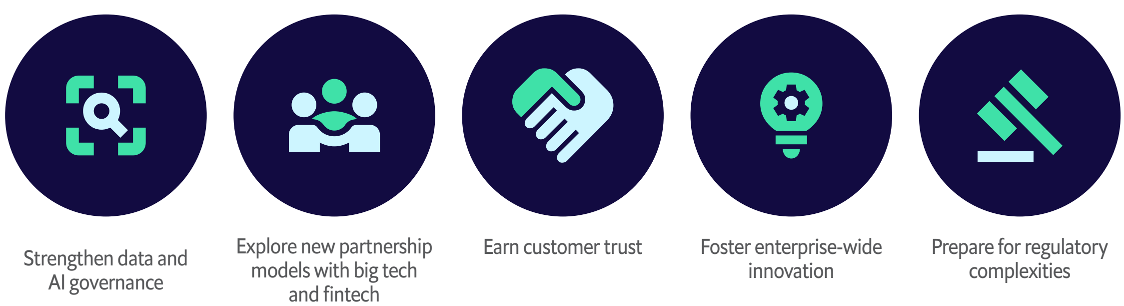
- **Traditional banks are expected to pose the weakest competitive threat in the industry over the long term.** Myriad threats are chipping away at their dominance as digital-only banks, fintech firms and big-tech companies continue to gain market share. Central-bank digital currencies (CBDCs) are also seen as potential disruptors, although their impact may take time to materialise.

- **Partnering with fintech and big-tech firms is a leading strategy for driving banking innovation, but poses data security risks.** These collaborations range from joint product development to integration with partner platforms. They are key to expanding digital banking ecosystems and embedded finance—the most significant revenue opportunities beyond core banking. However, 43% of executives cite data sharing with third parties as the top security concern. Adopting new partnership models with unified governance structures can help mitigate risks and ensure success.

- **Beyond partnerships, banks prioritise internal innovation over acquisitions.** Leveraging cutting-edge technologies for product development and fostering a culture of continuous learning among employees ranked above acquiring fintech firms as the most effective innovation strategies. Combined, they signal a preference for innovating internally, which can include building custom solutions such as chatbots and AI assistants. Particularly with genAI, preparing the workforce for enterprise-wide adoption should be central to a bank's innovation strategy.

Banks that master the complexity of this new banking environment are most likely to succeed. Facing intensifying competition, they are exploring new partnership models—not just with fintech and big tech, but also with vendors—to access innovative solutions, expand their reach and diversify their revenue streams. Operationalising successful genAI initiatives and experimenting more strategically on revenue-generating use cases will set them apart. Managing this within governance structures that are future-proof—enabling AI solutions today while supporting tomorrow's innovations—will drive business resilience and customer trust. In this way, instead of merely responding to disruptions, banks themselves can become disruptors.

The banking playbook



A time of transition: adapting to technology, tensions and risks

Technology advances, macroeconomic volatility and geopolitical instability are all reshaping the banking industry, as highlighted in our report *Banking in 2035: three possible futures*.[1] Tensions between global powers are contributing to rising financial fragmentation altering global capital flows.[2] Over the past few years, interest rates have experienced significant volatility, surging and then declining again, but remaining higher than pre-pandemic historic lows. These rapid fluctuations over a relatively short period of time exposed banks to liquidity risks, through higher funding costs and a decline in the market value of long-term fixed-income securities. Additionally, high interest rates and rising living costs are increasing consumer debt and eroding savings. For banks, this means high customer churn, shrinking deposits, and elevated credit and default risks.

The current banking era is also characterised by significant technology-driven innovations. AI and blockchain are streamlining operations, improving fraud detection and personalising customer experiences. Almost 80% of banking executives surveyed cite these technologies as the most disruptive forces of the next decade. This sentiment is even stronger in emerging markets such as Brazil (85%).

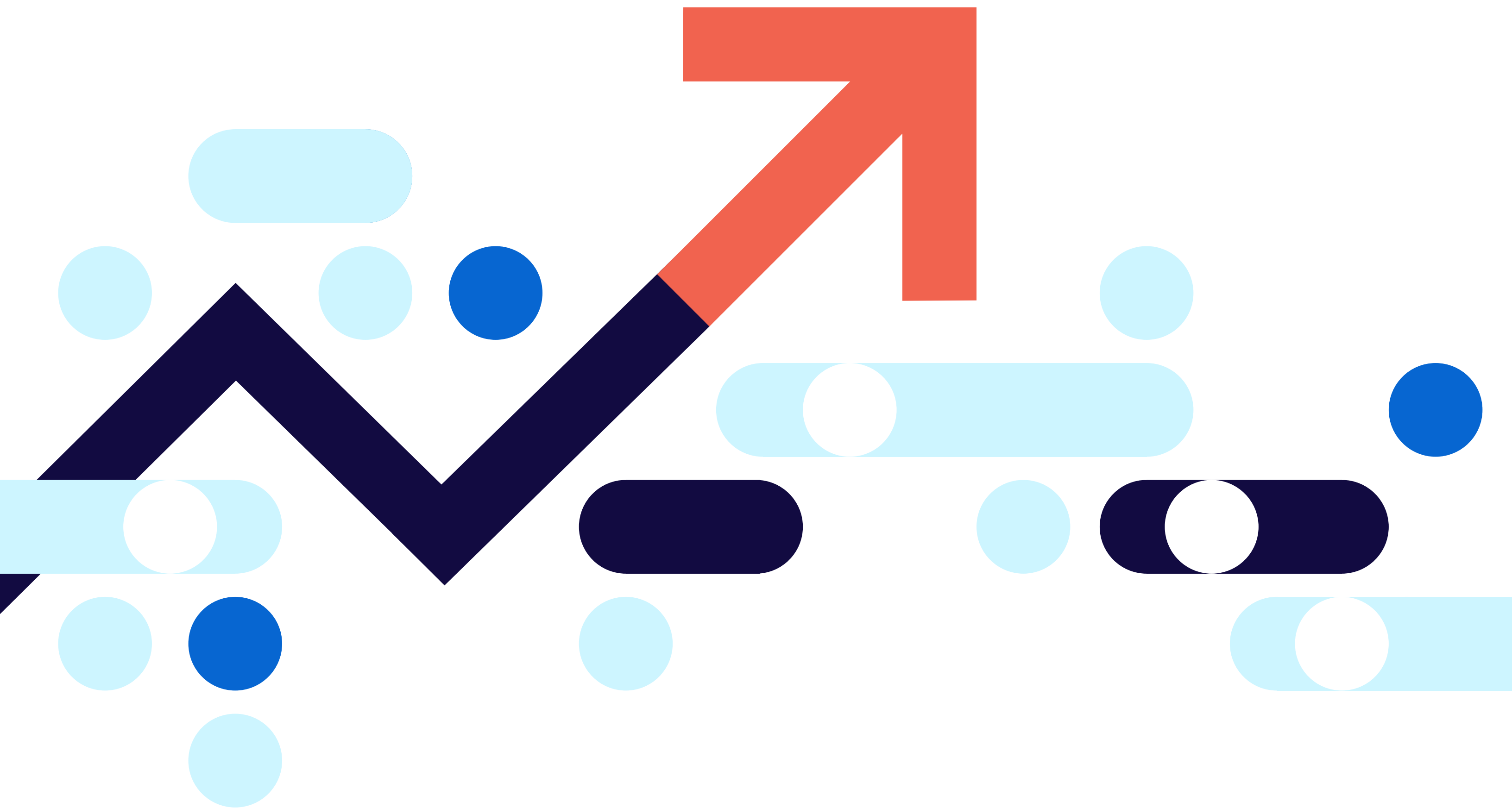
But executives also see major risks accompanying the integration of new technologies, including regulatory challenges and ethical concerns. Nearly 80% of banking executives expect cyber-attacks, fraud and financial crime to have a major impact on their institutions. The financial sector was the second-most targeted industry in 2024, accounting for 22% of total data breaches (down from 26% in 2023).[3] Money laundering amounts to between 2% to 5% of global GDP (about US$2trn to US$5.5trn in 2024 prices).[4] It supports various crimes including human, arms or drugs trafficking, with consequences well beyond the banking industry.

Importantly, the growing use of advanced technologies poses a risk to banks' most valuable asset: customer trust. All customers can potentially be affected by biases embedded in AI models, but vulnerable groups—such as minorities and the elderly—face greater risks of discrimination.[5, 6, 7] Those with limited digital footprints or non-native language proficiency may also face barriers to customer service. Missteps can be costly in terms of reputational damage and lost customers. Younger customers, who are more open to banking with multiple institutions and have plenty of alternatives, are especially sensitive to these issues.

Nearly 80% of banking executives expect cyber-attacks, fraud and financial crime to have a major impact on their institutions

In the face of an array of disruptive forces—and opportunities—banks are pursuing multifaceted technology strategies. As they embrace AI-driven automation to streamline operations and improve customer experience, they are also strengthening governance frameworks to protect customer relationships and prevent cyber-attacks. At the same time, they are forging partnerships with big tech firms and vendors of cutting-edge technologies to innovate faster, expand their reach and diversify revenue streams. Continuous employee training is taking on heightened strategic significance, ensuring that institutions are able to harness emerging technologies safely and effectively.

In a volatile age of rapid change, there is no single blueprint for success. But around the world, banking leaders share common goals as they leverage new technologies: to build resilience, increase efficiency, combat financial crime, improve the customer relationship and explore new opportunities through innovation.



AI and banking: balancing innovation and risk

Since the release of OpenAI's ChatGPT tool in November 2022, genAI has amassed far more attention than any other technology. However, in the banking industry (as in many others), there's no clear consensus on its potential near-term impact and value. Some see it as a game-changer that could unlock new levels of productivity and revenue, whereas others remain cautious due to operational and regulatory risks. What is clear is that almost all banks are experimenting with genAI in some form. As the initial hype wanes, the question leaders now grapple with is whether genAI can deliver real value.[8]

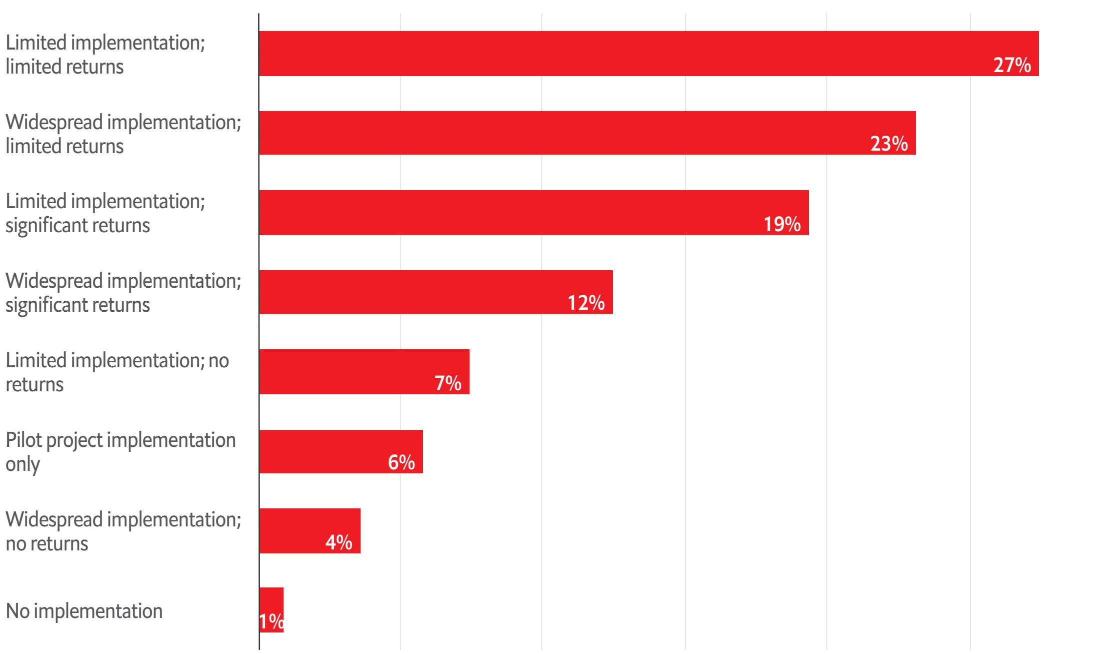
GenAI at a crossroads

GenAI adoption is widespread—almost all banking executives report some level of integration—but financial returns have fallen short. Just over half of executives (50%) report limited gains, and 11% see no returns at all. Fewer than one in five executives (19%) report significant returns from limited implementation, suggesting that targeted applications may offer higher rewards.

In 2025, banks will need to decide whether to scale up successful pilots or rethink genAI's role in solving business challenges. In some cases,

Figure 1: Value for money?

Percentage of respondents by extent of genAI adoption levels and returns



Source: Economist Impact survey

businesses are choosing the right tool, but using it for the wrong applications. As genAI's novelty wears off, the pressure to deliver tangible returns on investment continues to grow.[9] Prioritising revenue-generating and cost-saving applications can help drive returns.

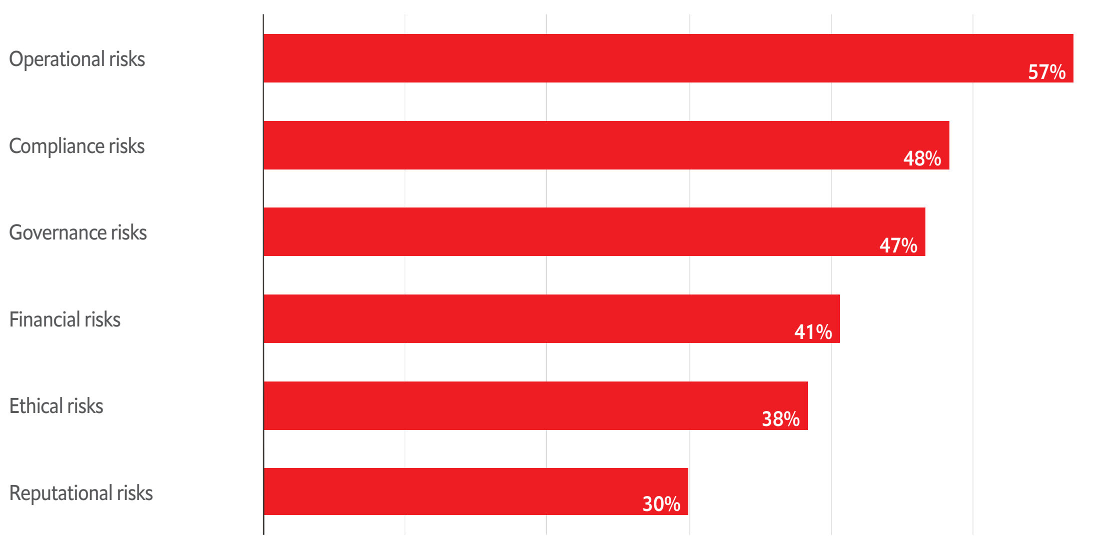
Broadly, however, there is agreement among industry experts that genAI could reshape the banking sector by enhancing efficiency, personalising customer experiences and improving fraud detection. "We're only really nibbling at the edges," says Thomas Wallace, chief risk officer at Revolut UK, a UK-headquartered digital bank. GenAI, he argues, could "democratise finance" by making tailored financial services accessible to more people, regardless of their assets or transaction volume.

But every technology introduces risks, and genAI is no exception. Operational and compliance risks are the top two concerns surfaced by surveyed executives (see Figure 2). These potential risks include automation errors, job displacement and regulatory violations due to mishandled customer data. Additionally, the growing complexity of global AI regulation opens the door to non-compliance challenges, leaving banks in uncertain legal positions.

Executives express less concern about ethical and reputational risks. However, all it takes is one major AI failure for banks to experience the repercussions of eroded public opinion and trust. Potential biases in their AI models (which are often trained on customer data) could lead to biased decision-making in lending or exposed personal information via data breaches, for example.

To address and mitigate these risks, banks are strengthening AI governance frameworks, ensuring human oversight of applications with integrated AI capabilities. These best practices, explored below, will play a critical role as the future of AI in banking comes into focus.

Figure 2: Walking the AI tightrope
Percentage of respondents most concerned about genAI risks



Source: Economist Impact survey

Case study: DBS's genAI-powered assistant speeds up customer service

Every month, DBS Bank's large team of customer service officers (CSOs) in Singapore receives more than 250,000 customer queries. One of Asia's leading financial institutions, the bank wanted to leverage genAI capabilities to ease the challenge of handling all these requests. So in 2023, the bank developed CSO Assistant, a genAI-powered tool designed to automate important aspects of the customer service workflow, such as call transcription, solution generation and service request handling. Its implementation has been a critical step in streamlining processes and improving response times, helping DBS meet rising customer demands and improve operational efficiency.

After the bank began piloting the CSO Assistant in October 2023, the tool has shown nearly 100% transcription and solution accuracy. CSOs using the tool have reported positive feedback, with 90% expressing satisfaction with its impact on their workflows. The assistant is expected to reduce call handling time by 20%, improving overall customer satisfaction and staff productivity. The initiative addresses growing demand for faster and more responsive customer interactions. The pilot's success has led DBS to implement the tool beyond Singapore, to support customer service teams in Hong Kong, India and Taiwan.

Importantly, the CSO assistant offerings were created within DBS's strategy designed to support the ethical use of AI. The bank's "PURE" framework ensures that AI use cases are "Purposeful, Unsurprising, Respectful and Explainable". The framework is supported by ADA (advancing DBS with AI) platform, which ensures centralised data governance, and ALAN (AI protocol and knowledge repository named after Alan Turing), which facilitates scalable AI model deployments.

GenAI can augment human capabilities, optimise workflows and enhance customer satisfaction. But achieving this is more likely with tailored solutions that address specific business challenges and can be seamlessly integrated with existing systems. DBS's CSO Assistant demonstrates the importance of targeted genAI implementation to achieve measurable operational efficiency in customer service operations.

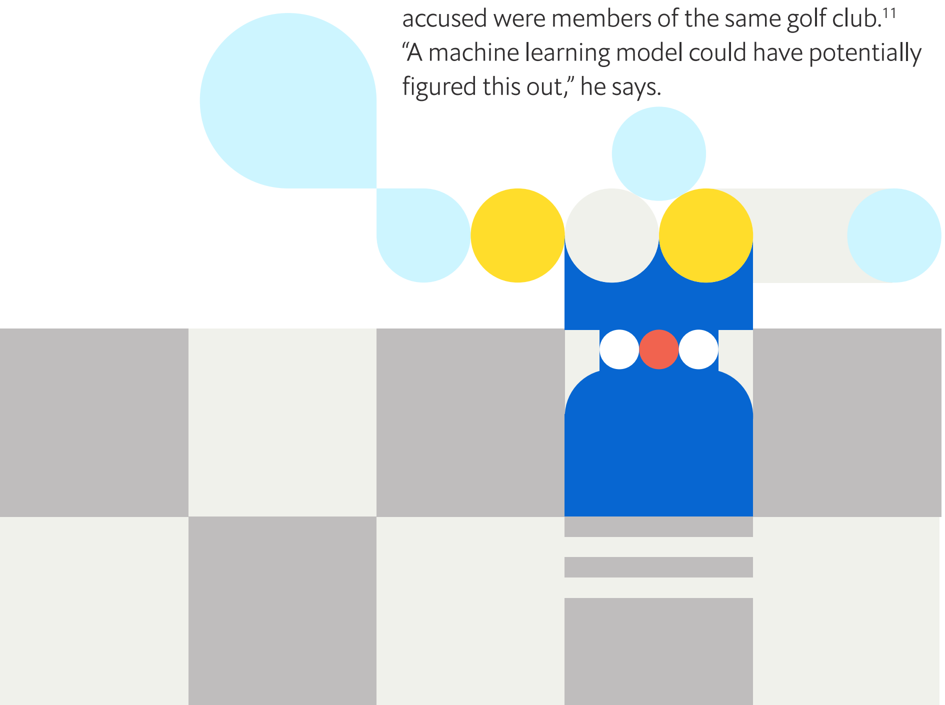
"Many top-performing financial institutions appoint an 'AI evangelist' in each single business function," he says. "[They] educate people, and that has proven useful."

Piotr Gonera, director of global corporate and investment banking, Mizuho Bank

GenAI and the fight against fraud

Financial institutions are combating rising identity fraud as scammers wield AI tools to create convincing fake credentials and deepfake media, making fraud tactics more sophisticated.[10] Indeed, 54% of surveyed banking executives cite their complexity as the biggest challenge. With consumer identities being prime targets, concern is higher among retail banks (59%) than corporate banks (54%). "We are in an arms race with fraudulent actors, and we hope to stay ahead," says Mr Wallace of Revolut.

In this fight, both sides are using genAI to gain advantage. In fact, AI can be a bank's most powerful tool for fraud detection, according to our survey respondents. "You really [need to] combine a lot of data to find fraudulent activities," explains Tobias Klingel, head of information security at Aspire, a Singapore-headquartered fintech firm. He recalls Singapore's largest-ever money-laundering case, which made headlines in 2024. Many of those accused were members of the same golf club.[11] "A machine learning model could have potentially figured this out," he says.



However, AI's high cost remains a barrier to widespread adoption. More than a third of surveyed executives said AI-powered detection is the most expensive strategy for fraud management. In addition to upfront investment, AI's energy-intensive computing adds to costs. However, banks can reduce expenses by using AI as a Service, a cloud-based solution that allows companies to use AI through third parties; open-source AI; or by embedding AI during product development.

Moreover, integrating AI solutions into existing fraud management systems can be a challenge, according to about half of the executives we surveyed. Many banks struggle with this because fraud detection and data analytics models rely on data that is scattered across the organisation, explains Piotr Gonera, director at Mizuho Bank, one of Japan's largest retail and corporate banks.

Strong AI literacy among business leaders is crucial to overcoming this, he adds. It deepens understanding of opportunities and risks, and enables informed decision-making. "Many top-performing financial institutions appoint an 'AI evangelist' in each single business function," he says. "[They] educate people, and that has proven useful."

35%

of surveyed executives said AI-powered detection is the most expensive strategy for fraud management.

Case study: A hybrid strategy for fighting fraud at Revolut

During the 2023-24 financial year, Revolut, a UK-based digital bank, was named in more financial fraud reports than any other UK bank.[12] To combat this, they deployed a multi-layered strategy that combines advanced technology, human oversight and customer education.

Revolut has made significant investments in AI-powered fraud detection, alongside traditional security measures enhanced by human review. The Payment Services (Amendment) Regulations 2024, which allow UK banks to hold payments they suspect to be fraudulent, has also become an effective tool in the company's fraud prevention arsenal.[13]

Another critical part of their strategy has been customer education. "We are arming our customers as the first line of defence," says Revolut UK's chief risk officer, Thomas Wallace. The firm integrates real-time fraud warnings within its app, using pop-up messages—such as before completing a transfer—to prompt users to pause and assess potential risks. "It helps them to almost slow down and make sure that what they're doing has been thought through," Mr Wallace says. This initiative aligns with the UK government's Take Five campaign, which promotes three core fraud prevention steps:

- Stop: pause before parting with money or personal information
- Challenge: question whether the request could be fraudulent
- Protect: report suspicious activity to the bank or authorities

To tackle impersonation fraud, Revolut introduced an in-app caller verification feature that allows customers to confirm whether an incoming call is genuinely from the bank. This enhances security and builds trust by reducing vulnerability to scams.[14] In early 2025, the company said impersonation scams affecting Revolut customers were at their lowest level in two years, despite the fact its customer base has grown substantially.[15]

A lesson for the broader banking sector is that technology alone is not enough. A hybrid approach to fighting fraud that blends AI, customer education and human oversight will build a safer banking experience.

"We are arming our customers as the first line of defence."

Thomas Wallace, chief risk officer, Revolut UK

Robust data governance requires a clear framework

AI tools derive much of their value from vast stores of data. So, if AI adoption is crucial to banks' technology transformation, so is data governance. More specifically, banks should establish a data governance framework: a formal set of policies and procedures a bank follows to protect the security and quality of data and ensure regulatory compliance.

"Having a strong governance framework is not optional," says Zechariah Akinpelu, chief information security officer at Unity Bank. "We have structured our AI oversight with a chief data officer, a dedicated compliance team and rigorous audits to ensure we meet regulatory standards while staying ahead of technological advancements." (See Table 1 for best practices.)

Survey results underscore the importance of data governance frameworks across the sector. A third of executives say that establishing such frameworks is the most effective strategy for data security—significantly higher than data management automation (25%) and AI-driven cyber threat detection (20%).

Robust governance also helps banks reduce risks related to privacy breaches, fraud and regulatory non-compliance. As AI evolves, ensuring compliance with shifting legal and ethical standards across jurisdictions is essential (and explored in the next section of this report). But, with few formal regulatory guidelines on ethical data use, some banks are setting their own standards.

Singapore's DBS Bank, for example, created the PURE framework—purposeful, unsurprising, respectful and explainable—to guide responsible

Table 1: Essential features of a robust data governance framework for banks

Category	Description
Ownership and accountability	Define roles such as chief data officer, data custodians and data owners, and assign clear responsibilities for data quality, integrity and compliance.
Data storage	Create a centralised data catalogue to store metadata, definitions and access policies.
Access controls and data security	Implement role-based access control, ensure data encryption (at rest and in transit) and secure Application programming interface (APIs) for data sharing.
Data sharing and interoperability standards	Align data formats across departments and establish APIs and secure data-sharing protocols to enable collaboration between departments and third parties.
Data provenance	Track data origins, transformations and usage to improve traceability, which is essential for audits and AI model explainability.
Data quality	Automate data anomaly detection and create dashboards for real-time quality monitoring.
Model management	Monitor AI model output continuously to detect drift and bias.
Regulatory compliance dashboard	Real-time tracking of compliance such as with General Data Protection Regulation (GDPR) etc.
Incident response plan	Fraud and anomaly detection systems and clear data breach notification protocols.
Ongoing training	Regular training for employees on data governance policies and AI ethics, fostering a culture of cross-functional collaboration.

Source: Economist Impact

> **"Just because we may be legally allowed to use the data and have the technology to [be able to], that does not mean that we should."**
>
> Nimish Panchmatia, chief data and transformation officer, DBS Bank

data use. "Just because we may be legally allowed to use the data and have the technology to [be able to], that does not mean that we should," says Nimish Panchmatia, chief data and transformation officer at DBS. A robust data governance framework can support the responsible deployment of AI solutions (see Standard Chartered case study) and prepare the bank for future innovations, such as quantum computing.

Along with security and compliance, governance frameworks can improve data quality by clarifying ownership, securing access and enabling traceability, ensuring data is accurate, compliant and reliable. About 41% of retail banking executives cite data quality as one of the main concerns for their business, compared with 28% in corporate banking, which could reflect the former's high volume and diversity of consumer data.

Ultimately, a sound framework will not only ensure compliance but sharpen the quality of decision-making across the organisation. Banks that invest in effective data frameworks today will be better placed to innovate responsibly—and outpace rivals tomorrow.

Figure 3: Best practices for responsible AI implementation & consumer data privacy control

Source: Economist Impact research

Case study: Standard Chartered's framework for responsible AI

As AI adoption gained traction in the banking sector, Standard Chartered faced a challenge: balancing innovation with compliance and risk management. The UK-based multinational bank's solution was to develop the Responsible Artificial Intelligence Standard. This was designed to mitigate AI model bias risk, ensure transparency and withstand regulatory scrutiny to safeguard customers and partners.

These principles are more than just words on paper. The bank enforces the standard through dedicated governance bodies. The Responsible AI Council oversees AI integration, ensuring their deployment of AI-powered technologies adheres to ethical and operational standards. The Digital Asset Risk Committee monitors emerging technologies, including digital assets, ensuring compliance with regulations and ethical guidelines.

Standard Chartered points to a variety of use cases supported by its AI framework:

- The bank monitors and analyses AI models to ensure fairness in credit decisions
- AI-driven decisions come with explanations accessible to both customers and regulators, fostering trust and accountability
- The bank's in-house SocialAI model identifies women-owned businesses within its client portfolio, allowing it to tailor financial products and services that better support female entrepreneurs, promoting financial inclusivity

Additionally, Standard Chartered collaborates with regulators to shape technical guidelines for AI models. To build trust in its AI models, the bank developed FRIDAY (framework responsible for intelligent data and algorithm yield), aligned with the Monetary Authority of Singapore's principles of fairness, ethics, transparency and accountability. FRIDAY improves risk management and decision-making and ensures AI models are interpretable, free from bias and compliant with regulations. Since its implementation, FRIDAY has reduced AI model review times by 60% and cut development turnaround time by 30%, demonstrating its effectiveness in improving decision accuracy and streamlining compliance.[16]

Banks should note the potential value of working closely with regulators and industry bodies to build strong governance frameworks. Innovation and principled control and compliance efforts can go hand in hand.

Opportunity in a regulatory maze

A recent cover of *The Economist* focused on the "revolt against regulation" as governments seek to dismantle rules seen as costly to enforce and offering limited benefits.[17] Yet even as some regulation may be scaled back, debate around the appropriate extent of new regulations affecting banks—particularly on the use of AI and other advanced technologies—continues.

The current AI regulatory landscape is similar to that of privacy laws: a patchwork of inconsistent and sometimes complicated rules. Multinational financial institutions are grappling with fragmented compliance standards in different regions and countries. The European Union's Artificial Intelligence Act classifies AI-driven financial decision-making as high risk, requiring strict data governance, transparency and human oversight. Meanwhile in America, state-level laws multiply[18] as the federal government fails to enact AI regulations that would apply nationwide.[19]

The conventional view has been that business leaders oppose regulations because they stifle growth and innovation, while adding new compliance costs. However, the reality is that most banking leaders just want consistency. "What we really need is clear frameworks for the use of technology within financial services," says Mr Wallace of Revolut. "That doesn't mean regulating it out of existence, it just means giving some good guardrails, making sure that everyone's following the same standards."

Moreover, the 68% of surveyed banking executives see new regulations on AI, blockchain and open banking as potential drivers of innovation, rather than barriers. Retail bankers, in particular, are optimistic about open banking rules. Nearly a third of leaders in this segment view them as an opportunity, compared to just 20% of corporate bankers.

However, most banks are contending with rising compliance costs—reported by more than 75% of the executives we surveyed. What is surprising is that two-thirds believe these costs are justified; the risks of noncompliance, which include fines and operational vulnerabilities, are not worth taking.

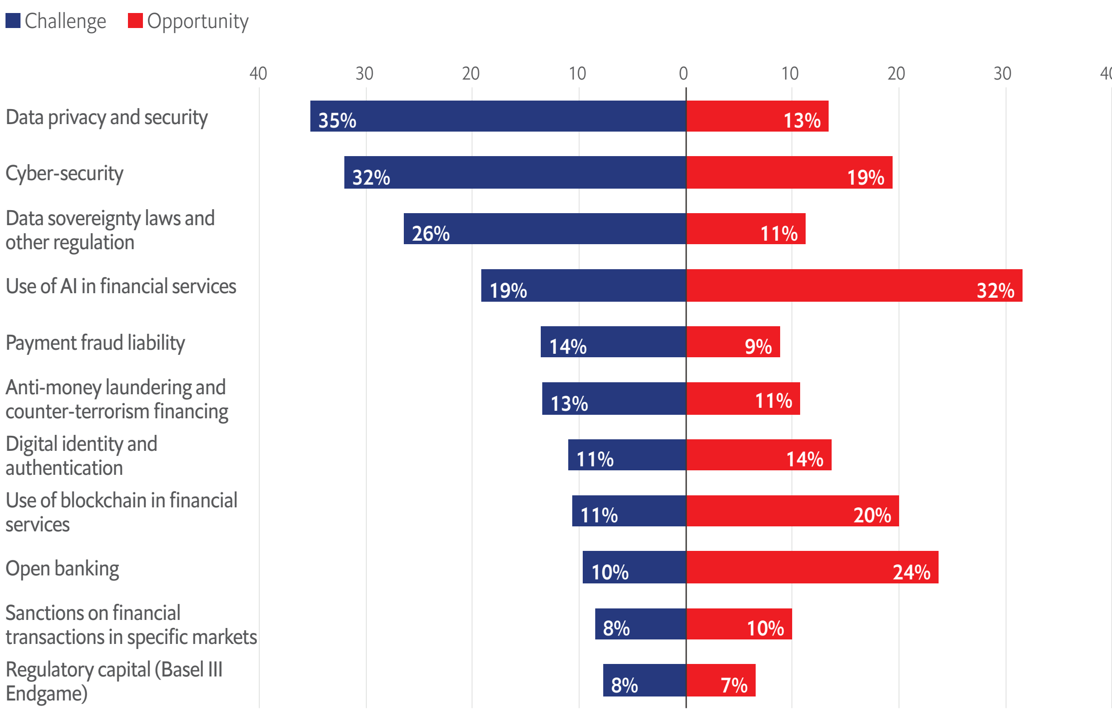
The executives we surveyed highlighted three areas they expect to be hardest to navigate over the next decade: data privacy, cyber-security and data sovereignty regulation (see Figure 3). As technology evolves and geopolitical tensions grow, legal frameworks for data privacy and sovereignty are expected to diverge, requiring banks to manage a multitude of laws across markets.

"What we really need is clear frameworks for the use of technology within financial services. That doesn't mean regulating it out of existence, it just means giving some good guardrails, making sure that everyone's following the same standards."

Thomas Wallace, chief risk officer, Revolut UK

Figure 4: Regulatory crossroads for banking

Percentage of respondents that cite regulation as an opportunity or challenge over the next decade



Source: Economist Impact survey

Banks cannot afford to be complacent about these regulations; beyond penalties, breaking these rules would have a direct impact on customer trust and retention.

To prepare for change, banks are investing in technology to automate compliance, reporting and risk monitoring. This is seen as the most effective strategy by more than a third of survey respondents, but it is also the most expensive. Periodic compliance audits, highlighted by survey respondents as the second-most effective strategy, offer a lower-cost alternative.

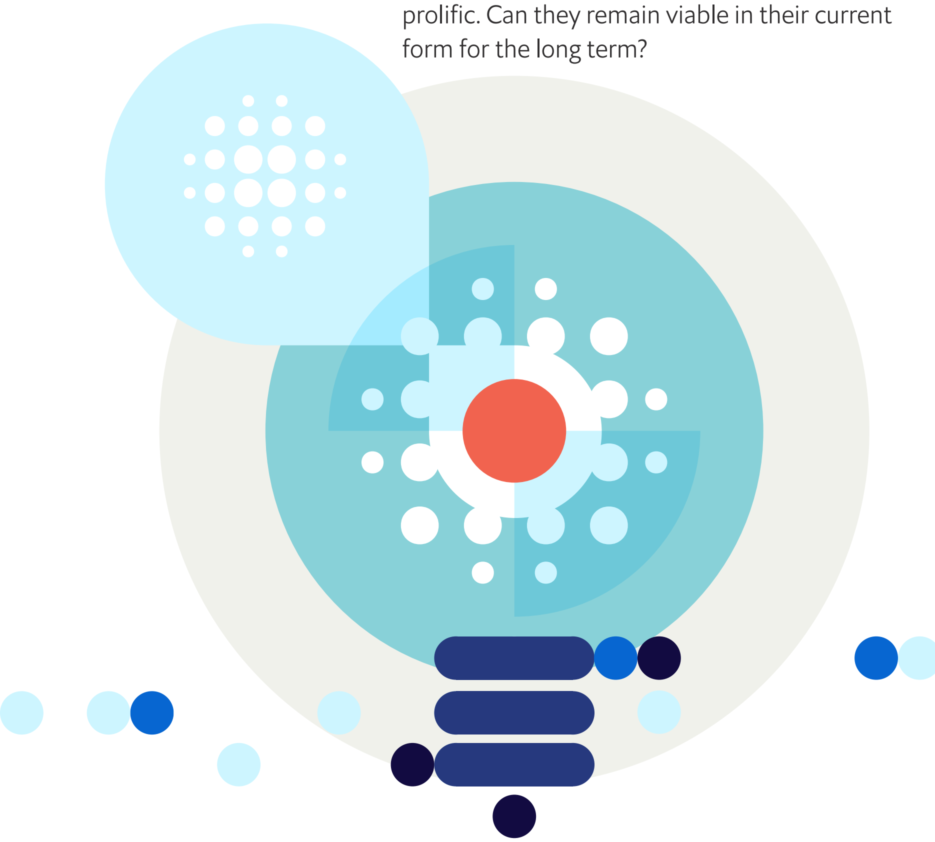
Enabling cross-department collaboration is one of the least costly strategies, but can be effective. Expanding into new markets with divergent regulatory requirements requires compliance and technical teams to work together closely. However, their respective priorities often clash. "Technical teams only want to build functionality and compliance teams want to fulfil local regulatory requirements," says Mr Klingel from Aspire. To bridge the gap, Aspire has structured teams with varying levels of technical and compliance expertise, ensuring smooth communication while maintaining regulatory standards.

As financial technology continues to evolve at an unprecedented pace, regulators are struggling to keep up. Some question whether true data privacy is even possible in an era of AI-driven financial services. But with growing consumer awareness of rising fraud risks and concern about AI, demand for strong data protection is higher than ever. However, banks are unlikely to see consistent rules across major markets any time soon. Instead, leaders must prepare to navigate an increasingly complex regulatory landscape while also looking to seize new opportunities to innovate.

The innovation imperative: banking's next frontier

Tens of thousands of fintech firms have launched over the past 15 years, bringing digital-first innovations and agility to the world of banking. Although the rate of new firm launches has slowed in recent years, fintech companies are steadily gaining market share, especially in emerging markets and in areas like digital payments. But even as digital upstarts gain full banking licenses—or become the most valuable bank in Latin America, as Nubank did in 2024—traditional banks have other disruptions to worry about. Big-tech firms are expanding into financial services through mobile wallets, and central-bank digital currencies (CBDCs) could eventually bypass banks altogether.

Although traditional banks still dominate financial transactions and core services like savings and lending, the existential threats they face are prolific. Can they remain viable in their current form for the long term?



Banking executives feel the pressure of growing competition. Although our survey respondents view traditional banks as the most disruptive source of competition in the short term, their competitiveness will drop sharply (see Table 2). Executives see digital-only banks, fintech firms and big tech as their biggest competition in the long term. These disruptors are leveraging technology to redefine customer expectations, streamline financial services and introduce innovative business models.

Recent developments signal a potential revival for the cryptocurrency sector. The US, a market leader, now is planning to create a strategic Bitcoin reserve and is enacting new stablecoin regulations.[20] For banks, this could mean greater competition, particularly for those reliant on money transfers. They may feel pressure to expand crypto services, such as custodial accounts, crypto lending or stablecoin payments. Given the volatility of digital assets, this would need to be accompanied by strong risk-management practices.

Interestingly, our survey results reveal that in the long term, executives are more concerned by CBDCs than any potential threats posed by other non-bank entities such as telecommunications companies. CBDCs could fundamentally alter the banking system. If widely adopted, they would allow individuals and businesses to hold accounts directly with central banks, reducing deposits, limiting lending capacity, and eroding banks' role in foreign exchange and international settlements. Some executives believe this shift will take years to materialise. But, if they take full flight, CBDCs could disintermediate banks on an unprecedented scale.

Table 2: Ranking of the most disruptive sources of competition

Rank	Short term (1-5 years)	Long term (6-10 years)
1	Traditional banks	Digital-only banks and other fintech firms
2	Digital-only banks and other fintech firms	Big tech companies (including super-apps)
3	Big tech companies (including super-apps)	Central-bank digital currencies
4	Third-party financial solution providers through open banking	Third-party financial solution providers through open banking
5	Central-bank digital currencies	Other non-bank entities such as telecommunications companies and retailers
6	Other non-bank entities such as telecommunications companies and retailers	Traditional banks

Source: Economist Impact survey

In the face of new competitors that are not only improving service delivery, but redefining the nature of banking, banks must adopt new strategies, or even entirely new business models, to chart a secure path forward.

As the adage goes, past performance is no guarantee of future results. The same is true for established banks, which must embrace continuous innovation. This entails much more than just adopting new technologies: it demands a shift in leadership mindset, strategic upskilling of employees, more agile collaborations and upgrading technology infrastructure.

When banks and financial institutions aim to innovate, they tend to evaluate three distinct options, says Roisin Levine, head of UK & Europe bank partnerships at Wise Platform, Wise's global payments network. "Build, buy or partner. While all the approaches have their pros and cons, we believe that fostering innovation through partnerships is often the most beneficial approach," she says.

Banking executives agree, with a third of survey respondents citing partnerships with big tech and fintech firms as the most effective innovation strategy. Such collaborations can help banks expand customer reach, integrate advanced technology and improve financial inclusion by serving underbanked populations.

"Banks and financial institutions tend to evaluate three distinct options when they aim to innovate: build, buy or partner. While all the approaches have their pros and cons, we believe that fostering innovation through partnerships is often the most beneficial approach."

Roisin Levine, head of UK & Europe bank partnerships, Wise Platform, Wise

Figure 5: Examples of banking industry partnerships

JPMorgan Chase partnered with Klarna to offer instalment loans, enabling consumers to make purchases with deferred, interest-free payments (see case study)[21]

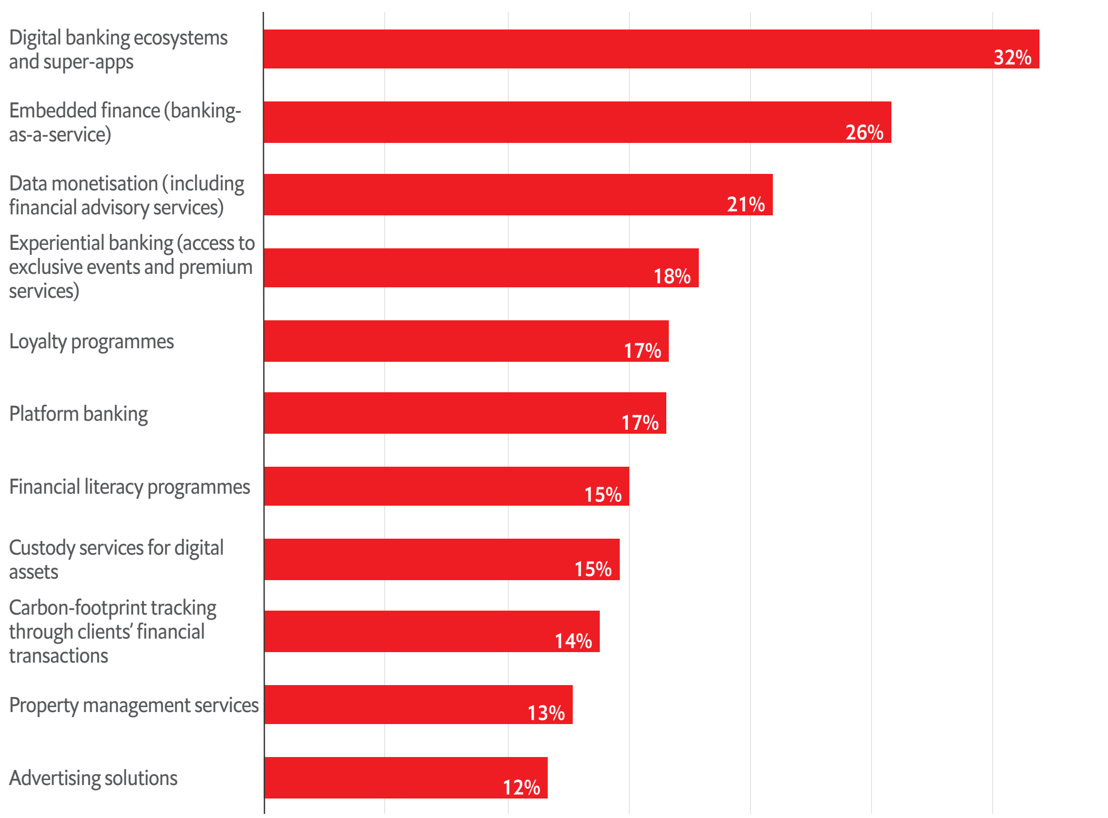
Amazon Mexico teamed up with buy now, pay later fintech Kueski to offer personal loans[22]

Standard Chartered worked with China's Ant Group to enhance cross-border trade financing using blockchain[23]

They can also unlock new revenue streams. Banks see digital banking ecosystems and embedded finance as the most promising opportunities outside core banking services, which can be enabled through partnerships with big tech and fintech. These firms provide APIs that allow banks to integrate financial services into non-financial platforms such as e-commerce sites, social media apps and ride-hailing services. Alternatively, banks can integrate with external services to create super-apps, as seen with Singapore-based DBS Bank's DBS PayLah!, which merges banking with lifestyle services.[24]

Figure 6: Ecosystem services will offer the biggest revenue opportunity beyond core banking services

Percentage of respondents citing the top two revenue opportunities



Source: Economist Impact survey

Revenue opportunities vary by region, with Asia and the Middle East indicating a slightly higher preference for digital banking ecosystems given their prominent super-app culture (both at 36%, versus 30% in Europe). In contrast, European banks favour embedded finance owing to the region's leadership in open banking regulation. Almost a third of respondents in Europe selected it as the top growth opportunity compared with 19% in Asia.

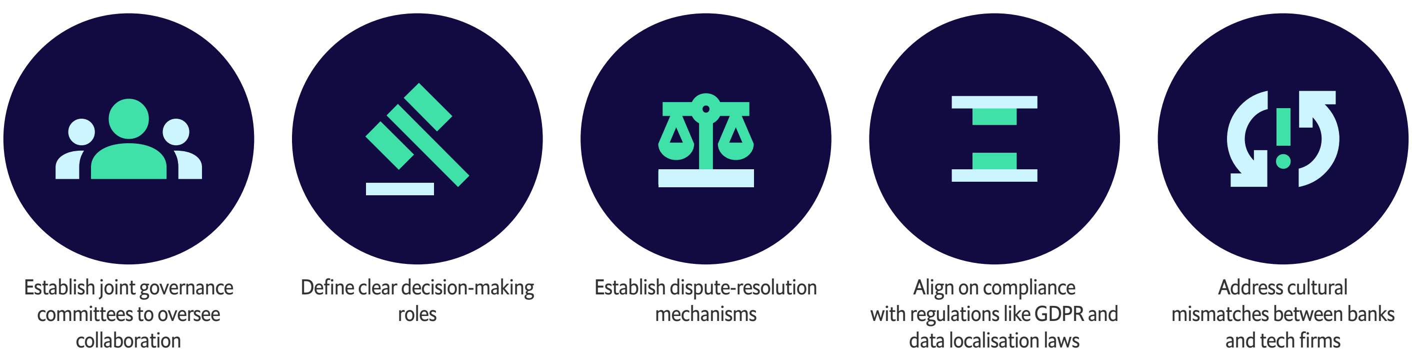
Although partnerships between banks and fintechs (and other non-bank firms) can foster innovation, they are not without risks, particularly regarding data security and governance. About 43% of executives cite data-sharing between banks, fintechs and third-party vendors as one of their top security concerns. Cyber-security measures and data management practices may not align between institutions, increasing vulnerabilities.

These strategic partnerships can also increase capital risk for banks. Third-party vendors and entities can broaden exposure to fraud and credit risk, as their KYC (Know Your Customer) checks may be weaker. Banks must ensure they have adequate capital buffers to absorb potential losses. Additionally, many big tech firms operate outside the jurisdiction of financial regulators, making it harder to assess risk exposure. The rapid expansion of these partnerships is already stretching regulatory oversight, with many agencies struggling to keep pace.

Despite the risks, partnerships between banks, big tech and fintech are likely to grow: the lure of new customers, novel technologies and fresh revenue streams may be too attractive to pass up. To ensure partnerships succeed, banks should employ a range of strategies, including establishing joint governance committees to align on compliance. The industry as a whole should also increase the use of collaborative frameworks that set common data security standards and best practices for third-party risk management. For example, the Financial Data Exchange (FDX) offers a framework that promotes secure and standardised data sharing in banking; 94m consumer FDX accounts were registered as of September 2024.[25]

As rapid change continues to transform the industry, banks that embrace strategic partnerships while effectively managing attendant risks will be more likely to thrive.

Figure 7: Best practices for partnerships



Source: Economist Impact research

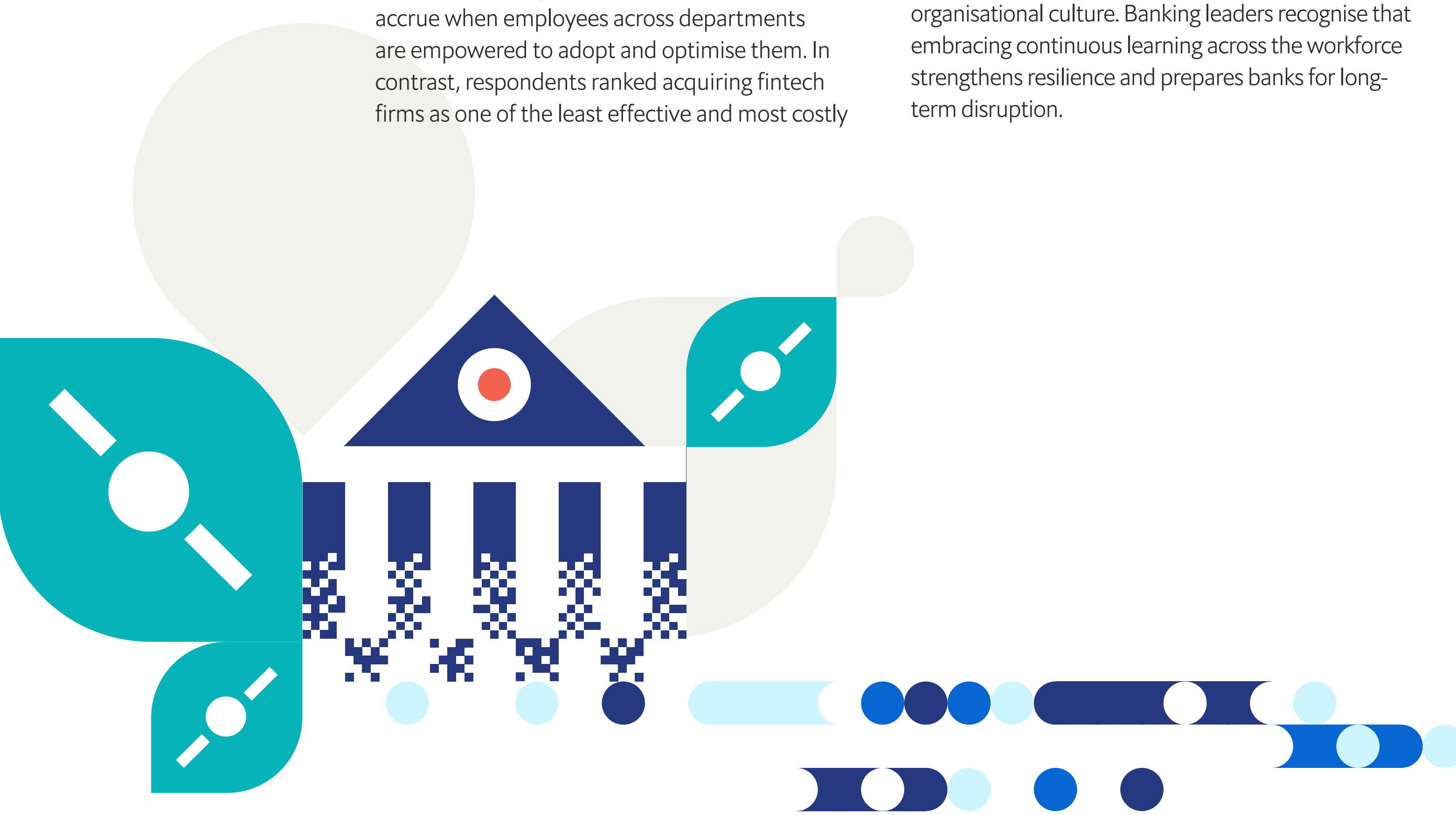
Drive innovation in-house or acquire?

As banking leaders seek to offer innovative new products and services, they face important decisions: what should be developed in-house, and what should be acquired? Acquisitions have long been a popular strategy. For instance, BNP Paribas's acquisition in 2023 of Kantox, a fintech firm specialising in currency management automation, allowed it to strengthen its position in digital financial services.

However, banking executives emphasise the importance of fostering innovation internally. Chief among their strategies are embracing cutting-edge technologies and promoting a culture of continuous learning and innovation. Combined, they signal a preference for building solutions in-house. Particularly with genAI tools, substantial benefits accrue when employees across departments are empowered to adopt and optimise them. In contrast, respondents ranked acquiring fintech firms as one of the least effective and most costly approaches, often due to cultural misalignment, regulatory hurdles and operational disruptions.

To support internal innovation, banks are investing in employee upskilling. Surveyed executives consider providing technology training for all employees or just leadership (cited by 36% and 30%, respectively) as the best ways to prepare the workforce for disruption, far outweighing hiring externally (cited by only 12%). This signals a clear preference for developing internal capabilities over relying on outside talent.

The two approaches are not mutually exclusive. Many banks may require both in-house development and selective acquisitions to achieve innovation goals. But ultimately, as technologies like genAI cause disruption and democratise innovation through increased access to knowledge, banks need to make innovation not only a strategic goal, but a core component of their organisational culture. Banking leaders recognise that embracing continuous learning across the workforce strengthens resilience and prepares banks for long-term disruption.



Case study: A win-win partnership blends blue chip bank and BNPL fintech

Buy now, pay later (BNPL) services have surged in popularity in recent years. In response, JPMorgan Payments, a division of JPMorgan Chase, sought to integrate BNPL offerings into its merchant services. The American bank made a strategic decision to avoid the costly and time-consuming process of developing a proprietary BNPL system and instead partnered with Klarna—a leading BNPL fintech company.

The resulting integration, launched in February 2025, embedded Klarna's payment methods, including interest-free BNPL and flexible financing options, into JPMorgan Payments' Commerce Solutions Platform. The strategic partnership offers the New York-based banking giant four major benefits:

- **Speed to market**
  Klarna's infrastructure allows JPMorgan to quickly deploy BNPL services without delays from regulatory approvals and system development. Additionally, Klarna's network includes 150m customers and over 500,000 merchants, reducing the need for JPMorgan to build its merchant network from scratch.
- **Risk assessment**
  BNPL offers short-term loans without traditional credit checks, which would require advanced risk modelling. Klarna has refined risk assessment algorithms, using AI and alternative credit scoring methods that JPMorgan does not specialise in. Rather than investing in homegrown risk models, JPMorgan can rely on Klarna's expertise to handle lending decisions.
- **Regulatory compliance**
  Klarna has built regulatory expertise relative to consumer protection laws across regions.
- **Operational efficiency**
  Klarna manages BNPL logistics, including loan servicing, credit reporting, fraud detection and customer support, allowing JPMorgan to focus on providing payments infrastructure.

There are many benefits for Klarna as well. The company gained access to JPMorgan's network of over 900,000 merchants, significantly broadening its market reach in America ahead of its planned initial public offering.

The lesson for the banking industry is clear: traditional banks can partner with fintechs to rapidly scale innovations, enhancing the payment experience for both merchants and consumers. In an era of rapidly changing consumer preferences, partnerships can power agility.

The banking playbook: five strategies for the future

Before the rise of intelligent financial systems, banks faced a choice between innovation or obsolescence amid the influx of fintech challengers. But now, with AI, blockchain and data-driven ecosystems redefining the banking sector, the risks of stagnating are much higher.

Transformational change is always accompanied by turbulence. Financial crimes are increasing, regulatory frameworks are in flux, and competition is intensifying from fintech firms, big tech and even central banks. To stay ahead, banks must prioritise the following five strategies.

Strengthen data and AI governance
- Implement robust governance frameworks to ensure data security and data quality, compliance and accountability.
- Deploy AI responsibly, with a focus on model integrity and ethics, to reduce errors and bias.
- Create an AI ethics committee and conduct regular audits to identify vulnerabilities and maintain compliance.

Earn customer trust
- Provide customers and partners with explanations of AI-driven decisions.
- Protect sensitive customer data with strong encryption and access protocols.
- Use AI to analyse customer sentiment and continuously improve services.

Prepare for regulatory complexities
- Automate compliance to streamline reporting and risk monitoring.
- Conduct periodic compliance audits to mitigate legal and financial risks.
- Enable cross-department collaboration to ensure regulatory alignment across business functions.

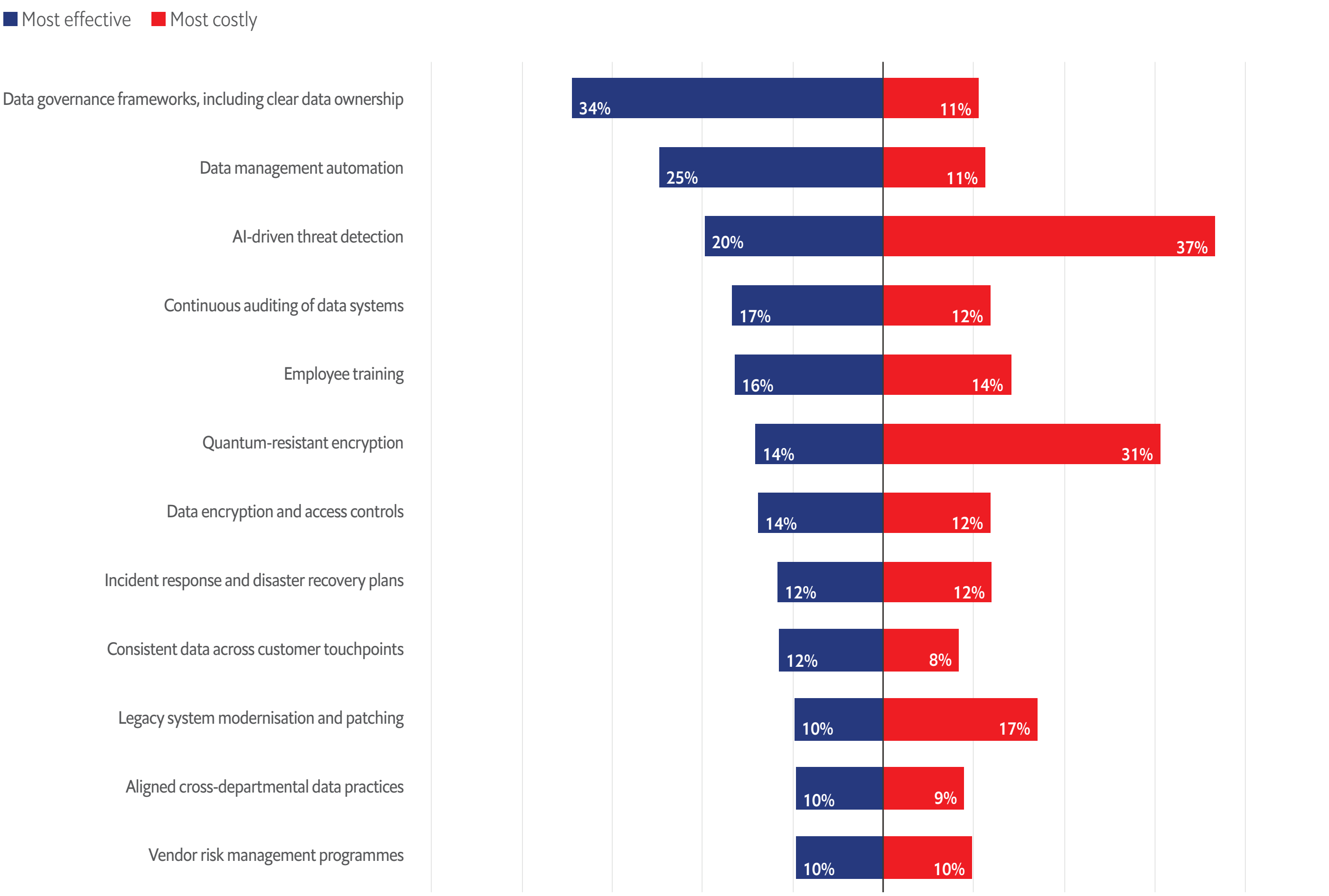
Explore new partnership models
- Leverage partnerships with fintech and big tech firms to drive innovation and embedded finance solutions.
- Establish joint governance committees to oversee data-sharing and compliance challenges.

Foster enterprise-wide innovation
- Invest in cutting-edge technologies and create a culture of continuous learning to enable employees across departments to contribute to banking innovation.

The companies that will thrive in the new era of intelligent banking will be those that master the complexity of new technologies. This will demand robust governance structures with clear human oversight of novel solutions. Innovation doesn't happen by accident; technology experts must create useful financial products and services, and valuable customer experiences, marking a shift from the previous approaches of traditional banks. With so many executives ready to embrace change, as this report underscores, there is hope that many banks will successfully innovate to compete with newer disruptors.

Appendix

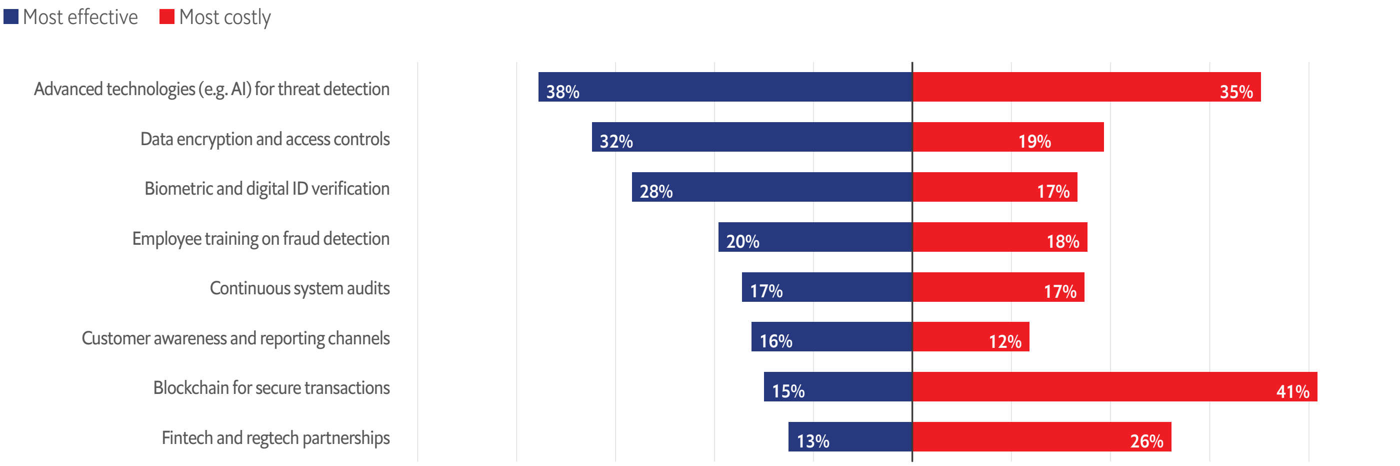
The most effective strategies to improve data management and security
Percentage of respondents



Source: Economist Impact survey

The most effective strategies for fraud detection and prevention

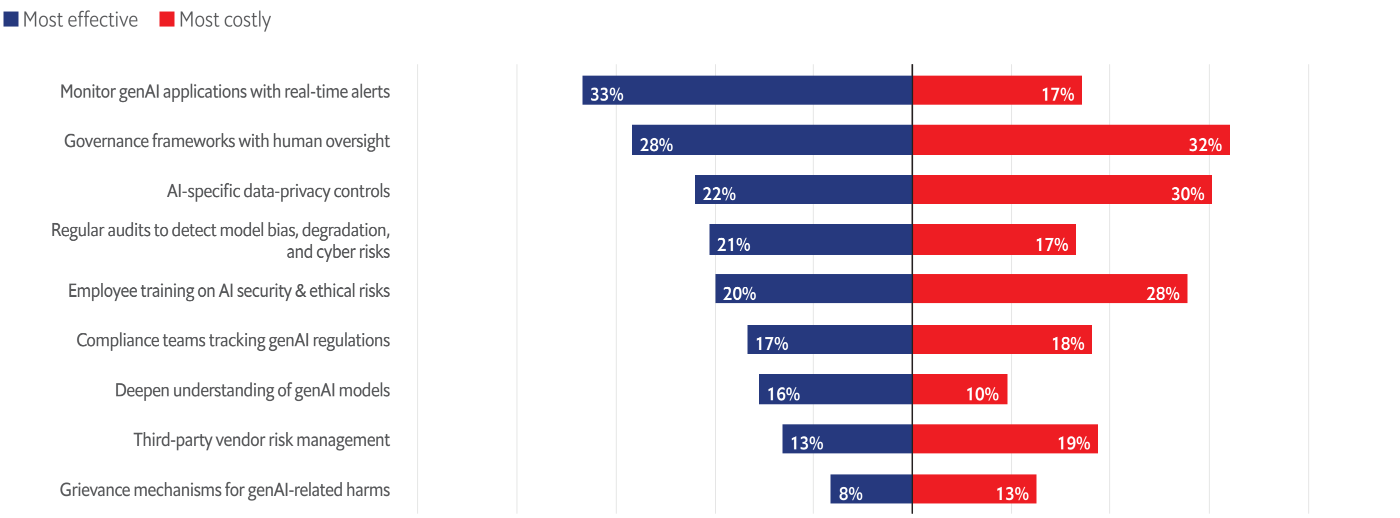
Percentage of respondents



Source: Economist Impact survey

The most effective strategies for enhancing the security of genAI applications

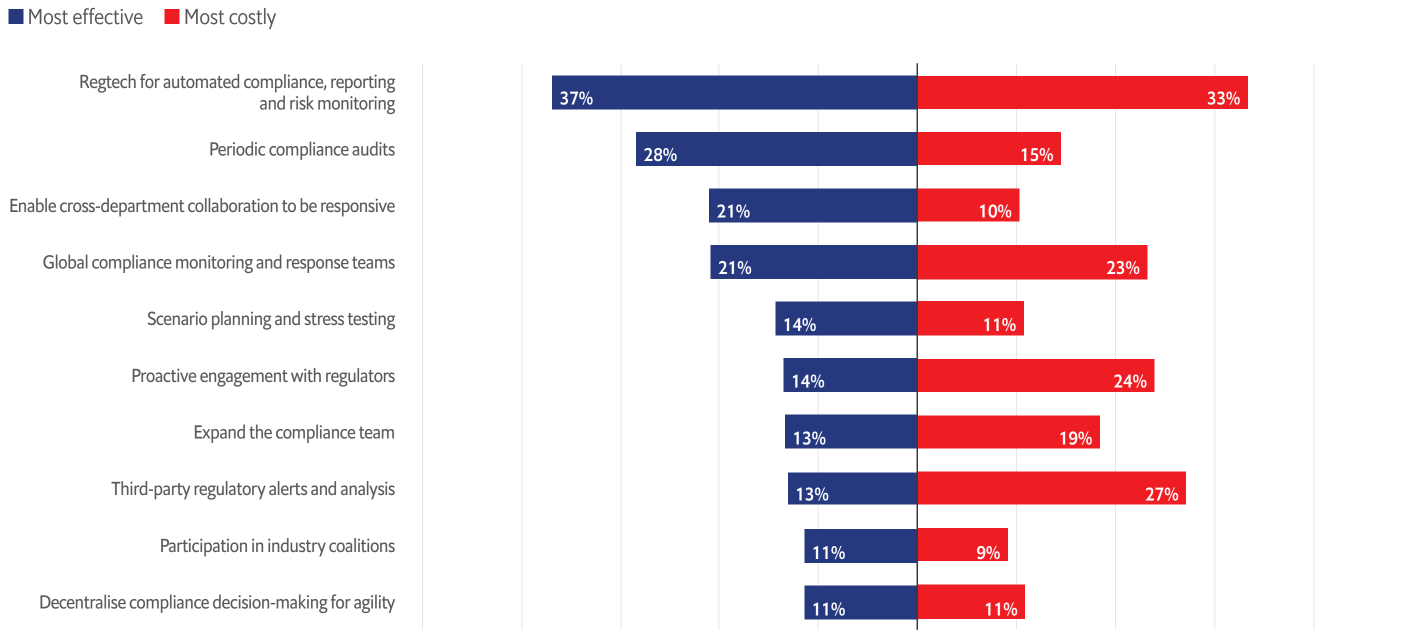
Percentage of respondents



Source: Economist Impact survey

The most effective strategies to prepare for and comply with regulations

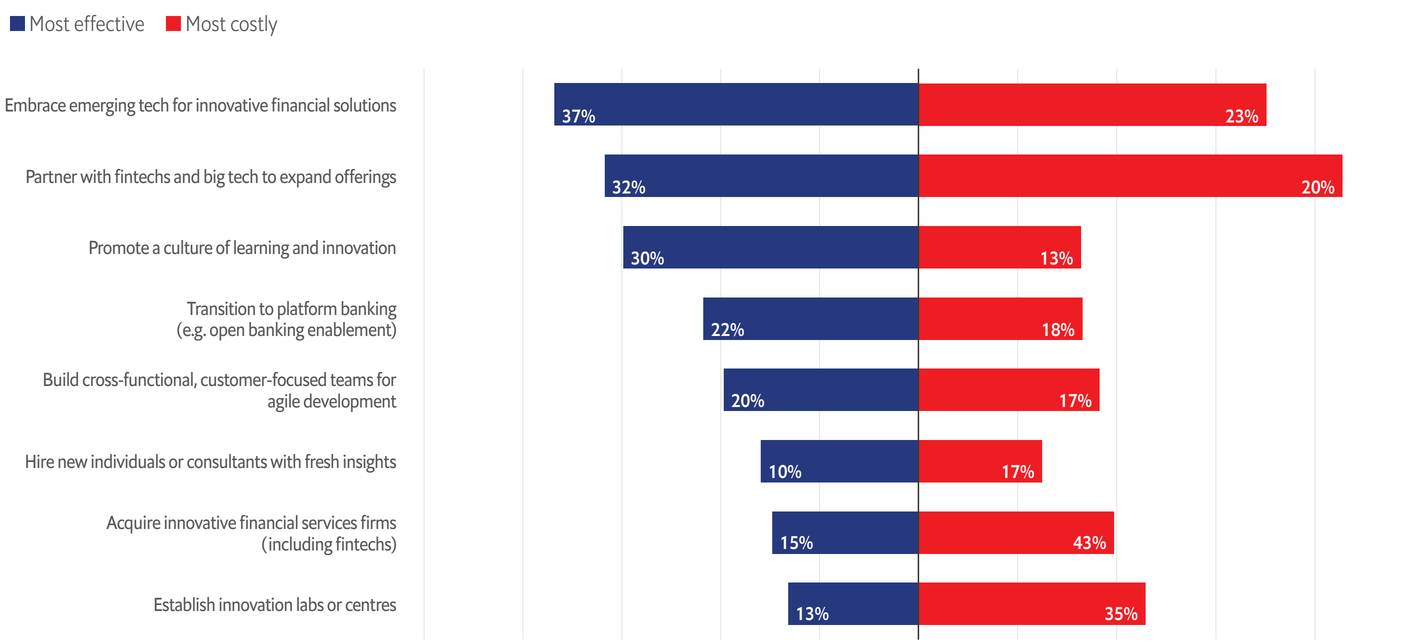
Percentage of respondents



Source: Economist Impact survey

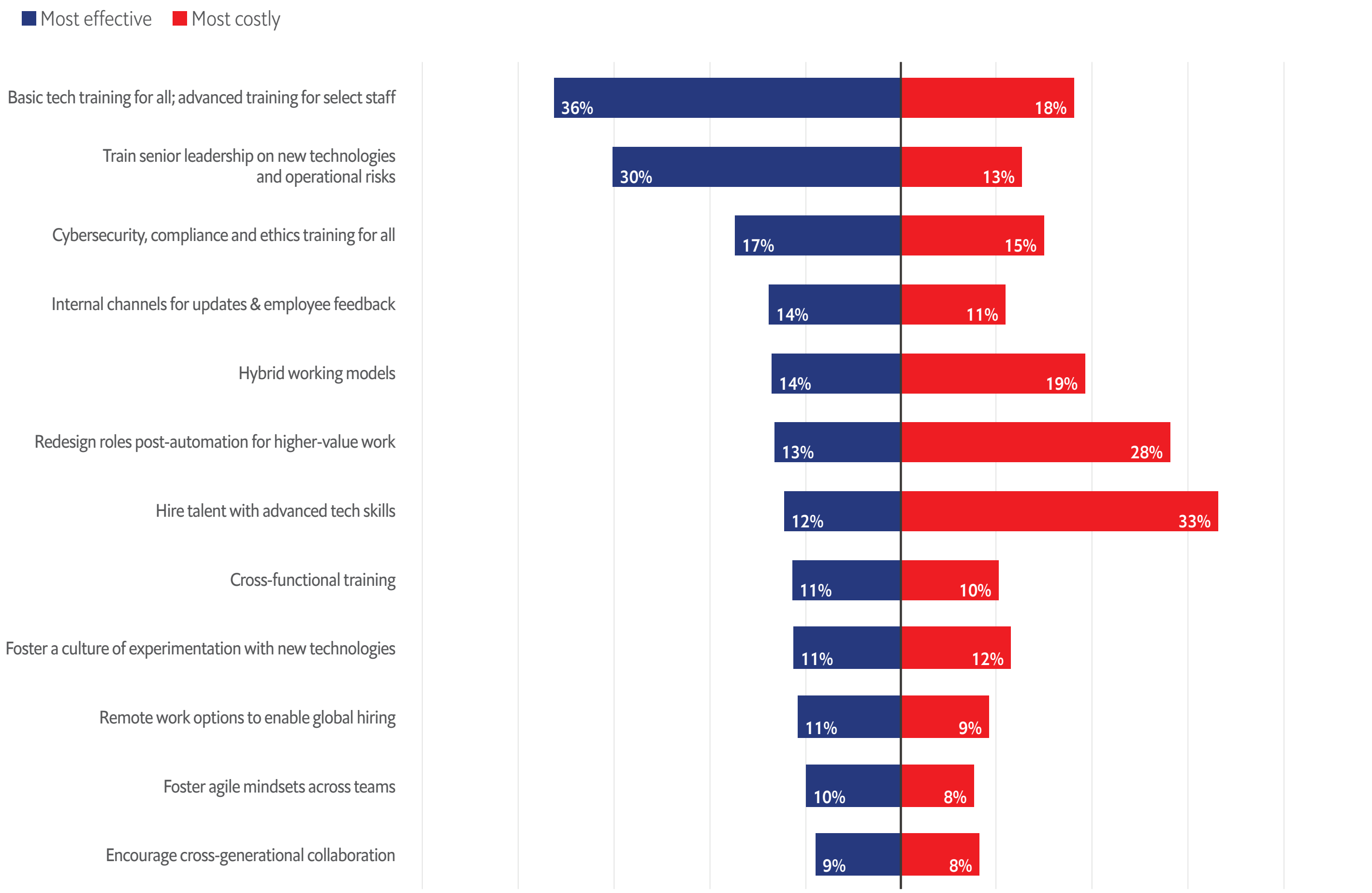
The most effective strategies to foster innovation

Percentage of respondents



Source: Economist Impact survey

The most effective strategies to prepare the workforce for disruption
Percentage of respondents



Source: Economist Impact survey

References

[1] Economist Impact, Banking in 2035: Three Possible Futures, 2024, Available at: https://impact.economist.com/perspectives/sites/default/files/banking_in_2035_three_possible_futures_briefing_paper.pdf

[2] World Economic Forum, Economic Fragmentation and Global Tensions: Experts Weigh In, 2024, Available at: https://www.weforum.org/stories/2024/06/economic-fragmentation-global-tensions-experts/

[3] Kroll, Data Breach Outlook 2024, 2024, Available at: https://media-cdn.kroll.com/jssmedia/kroll-images/pdfs/data-breach-outlook-2024.pdf?_ga=2.42187685.1235147258.1738248171-1855591750.1738248171

[4] United Nations Office on Drugs and Crime (UNODC), Money-Laundering Overview, Accessed February 2025, Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html

[5] EY, Banking Risks from AI and Machine Learning, 2024, Available at: https://www.ey.com/en_us/board-matters/banking-risks-from-ai-and-machine-learning#:~:text=Regulators%20have%20expressed%20concerns%20about,are%20also%20on%20authorities'%20radars.

[6] Forbes, AI Bias Caused 80% of Black Mortgage Applicants to be Denied, 2021, Available at: https://www.forbes.com/sites/korihale/2021/09/02/ai-bias-caused-80-of-black-mortgage-applicants-to-be-denied/

[7] The Guardian, Revealed: Bias Found in AI System Used to Detect UK Benefits, 2024, Available at: https://www.theguardian.com/society/2024/dec/06/revealed-bias-found-in-ai-system-used-to-detect-uk-benefits

[8] The Economist, Artificial Intelligence Is Losing Hype, 2024, Available at: https://www.economist.com/finance-and-economics/2024/08/19/artificial-intelligence-is-losing-hype

[9] McKinsey & Company, Superagency in the Workplace: Empowering People to Unlock AI's Full Potential at Work, 2024, Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

[10] Cyber Magazine, AuthenticID Report Shows Deepening Financial Sector Threat, 2024, Available at: https://cybermagazine.com/cyber-security/authenticid-report-shows-deepening-financial-sector-threat

[11] The Straits Times, Golf Club Managers to Meet Over Money Laundering Concerns Amid $1 Billion Probe, 2024, Available at: https://www.straitstimes.com/singapore/golf-club-managers-to-meet-over-money-laundering-concerns-amid-1-billion-probe

[12] BBC News, I lost £165k to fraud in an hour - customers say they were let down by Revolut, Available at: https://www.bbc.com/news/articles/cj6epzxdd77o

[13] UK Government, The Legislative Act: UKSI 2024/1013, 2024, Available at: https://www.legislation.gov.uk/uksi/2024/1013/body/made

[14] Revolut, Revolut Introduces In-App Calls to Help Customers Expose Phone Call Scams, 2024, Available at: https://www.revolut.com/news/revolut_introduces_in_app_calls_to_help_customers_expose_phone_call_scams/

[15] Ibid

[16] Singapore Business Review, Standard Chartered Stands Out in Marrying Trust & Artificial Intelligence (AI), 2024, Available at: https://sbr.com.sg/co-written-partner/event-news/standard-chartered-stands-out-in-marrying-trust-artificial-intelligence-ai?

[17] The Economist, Weekly Edition, 2025, Available at: https://www.economist.com/weeklyedition/2025-02-01

[18] TechPolicy Press, The Coming Year of AI Regulation in the States, 2024, Available at: https://www.techpolicy.press/the-coming-year-of-ai-regulation-in-the-states/

[19] Bloomberg Law, Companies Look to Jumble of AI Rules in Absence of US Direction, 2024, Available at: https://news.bloomberglaw.com/artificial-intelligence/companies-look-to-jumble-of-ai-rules-in-absence-of-us-direction

[20] S&P Global Ratings, Stablecoin Regulation Gains Global Momentum, 2024, Available at: https://www.spglobal.com/ratings/en/research/articles/250210-stablecoin-regulation-gains-global-momentum-13400761

[21] Klarna, Klarna Signs with J.P. Morgan Payments to Expand Merchant Services Offering, 2024, Available at: https://www.klarna.com/international/press/klarna-signs-with-j-p-morgan-payments-to-expand-merchant-services-offering/

[22] Fintech Magazine, Amazon Partners with Fintech Kueski for BNPL in Mexico, 2024, Available at: https://fintechmagazine.com/articles/amazon-partners-with-fintech-kueski-for-bnpl-in-mexico

[23] Standard Chartered, Standard Chartered Completes First HKD-Denominated Blockchain Test Settlement with Ant International's Whale Platform, 2024, Available at: https://www.sc.com/en/press-release/standard-chartered-completes-first-hkd-denominated-blockchain-test-settlement-with-ant-internationals-whale-platform/#:~:text=Through%20combining%20Standard%20Chartered's%20core,of%20Platform%20Tech%20at%20Ant

[24] DBS Bank, DBS PayLah!, 2024, Available at: https://www.dbs.com.sg/personal/deposits/pay-with-ease/dbs-paylah https://www.dbs.com.sg/personal/deposits/pay-with-ease/dbs-paylah

[25] Financial Data Exchange (FDX), FDX Hits 94 Million Accounts, CFPB Publishes FDX's Standard-Setting Application, 2024, Available at: https://www.financialdataexchange.org/FDX/FDX/News/Announcements/FDX%20Hits%2094%20Million%20Accounts,%20CFPB%20Publishes%20FDX's%20Standard-Setting%20Application.aspx

While every effort has been taken to verify the accuracy of this information, Economist Impact cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report.

The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

ECONOMIST IMPACT

LONDON
The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

NEW YORK
900 Third Avenue
16th Floor
New York, NY 10022
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

HONG KONG
1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

GENEVA
Rue de la Rôtisserie 11
1204 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

DUBAI
Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

SINGAPORE
8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com

SYDNEY
Level 14, Unit #138,
5 Martin Place, Sydney
Australia.
Tel: (61) 2 8551 0023
Email: asia@economist.com

GURUGRAM
Skootr Spaces, Unit No. 1
12th Floor, Tower B
Building No. 9
Gurugram – 122002
India
Tel: (91) 124 6409 300
Email: asia@economist.com