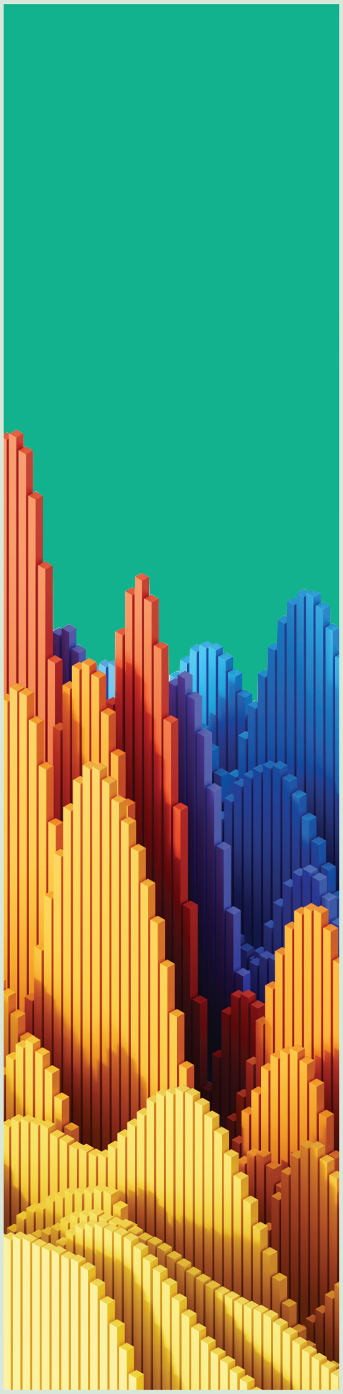
WHITE PAPER



INFOSYS BANK TECH INDEX VOL 5: KEY CLOUD ADOPTION TRENDS IN GLOBAL BANKING

Infosys®
Navigate your next

Cloud adoption is evolving at pace. As banks across the world accelerate their AI transformation programs, to drive innovation, streamline compliance and enhance customer experience, they are resetting their cloud strategies to support new business priorities and respond to a dynamic marketplace. In particular, intense scrutiny around data security and compliance is leading to more banks exploring private cloud solutions and hybrid models. They view this type of cloud repatriation as the easiest and safest route to balance innovation with risk management.

The Bank Tech Index Vol 5 highlights the extent to which banks are comfortable migrating their core platforms and customer data to the cloud but are still relatively hesitant about moving organizational data (such as financial information and Intellectual Property). Currently, only around a quarter of banks are hosting organizational data in the cloud, with leaders all too aware of the potential damage any breach in security of this data would bring. Significantly, however, banking leaders plan to dramatically increase their usage of cloud platforms over the next three years, for both core and non-core platforms, for customer data and organizational data. They expect that more than 90% of core platforms, non-core platforms and customer data to be hosted in the cloud by 2028, along with more than two thirds of organizational data. The shift to the cloud that we have witnessed over the last five years will continue unabated.

Cloud adoption will naturally evolve and mature at varying speeds across regions, largely due to different regulatory landscapes. This is most evident in attitudes to moving organizational data to the cloud. In North America we're likely to see a huge uplift in the number of banks migrating organizational data compared to in Europe and the Middle East and Africa.

Of course, the path to the cloud is never straightforward, and the research highlights a number of challenges that banks are encountering as they look to advance their cloud programs. This paper explores these barriers to progress and offers best practice guidance for banking leaders to navigate three of the major challenges cited in the research: data security and privacy, regulatory compliance, and cost management.

About the bank tech index

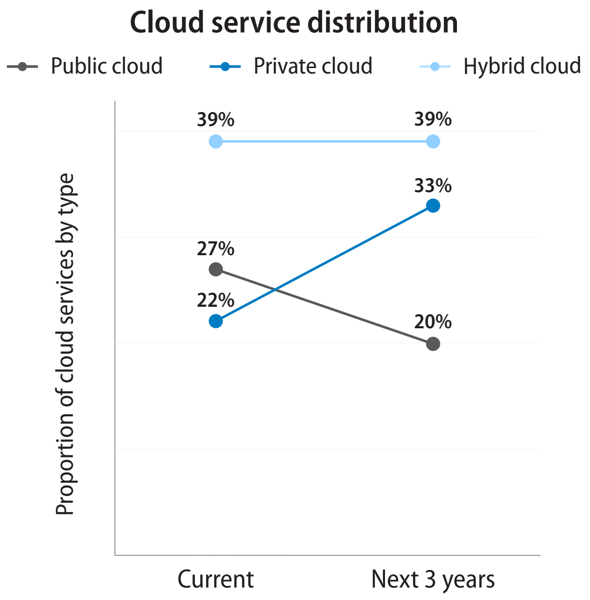
The Infosys Bank Tech Index is a semiannual, survey-based research report that indexes technology investment, adoption, and talent trends across the banking industry. The fifth edition gathers quantitative data from 400 of the largest banks by total assets in Asia Pacific, Europe, Latin America, Middle East and Africa, and North America. Our survey, exclusive to banks with assets surpassing $10 billion, represents 98% of this asset pool. This quarterly research gathers insights on technology spending, staffing, and performance from a panel of leading banks. Our executive panelists are key decision makers for their respective bank's technology investments and talent strategies.

The growing shift to cloud repatriation

Over recent years, banks have refined their cloud strategies in response to changing data security and privacy regulations, and to support the rapid acceleration of AI transformation programs. The research finds that nearly 88% of banks now have a cloud strategy in place and this figure is expected to rise to 92% by 2028. Across all regions, banks are increasingly deploying cloud (across public, private and hybrid) to drive operational efficiency and resilience and to advance their most important strategic objectives.

Significantly, the next three years are likely to see a trend towards cloud repatriation. The percentage of banks deploying private clouds is expected to rise from 22% to 33%, while consumption of public clouds will fall from 27% to 20% of banks. This shift towards private clouds is consistent with other industries and driven by the amplified need for organizations to balance scalability and flexibility with tighter security and regulatory compliance frameworks. Moving forward, banks will deploy private clouds for critical workloads and sensitive data, and use public clouds for less sensitive operations which require enhanced scalability.

Percentage of banks that use public, private and hybrid cloud today and in three years



1. N = 400, where N is the number of banks surveyed in Volume 5.

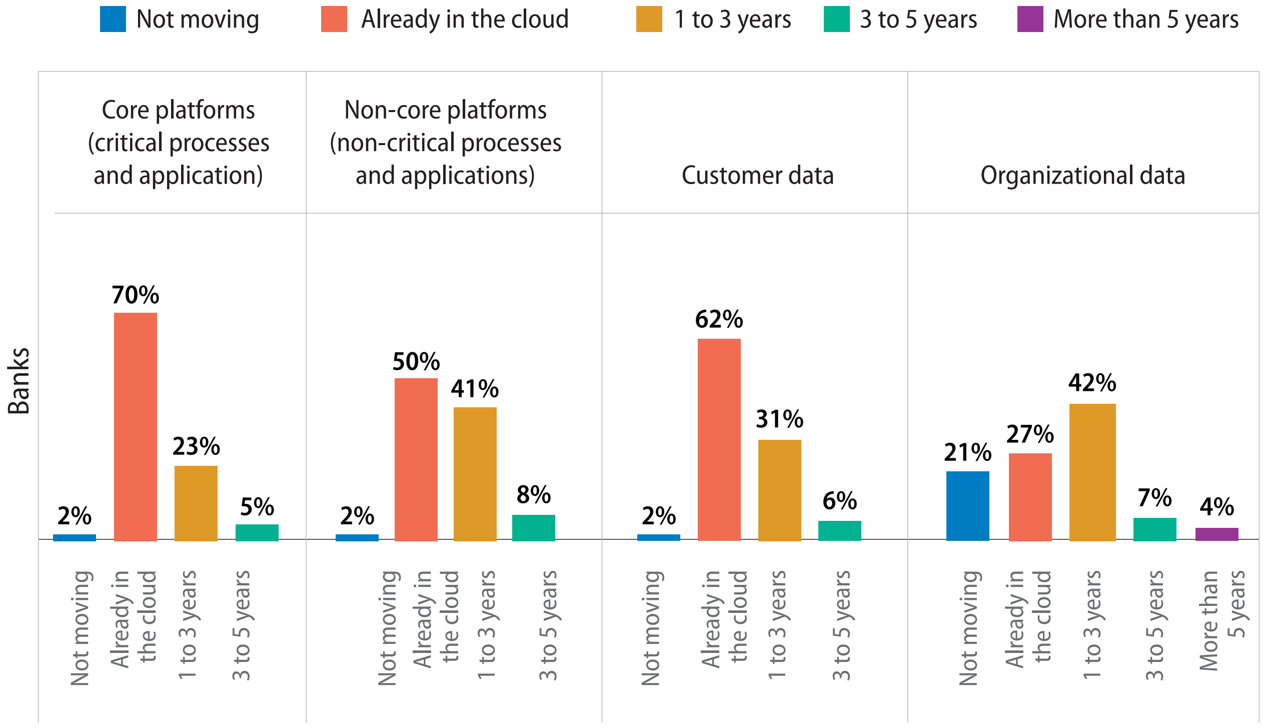
Banks are retaining organizational data in-house

Levels of comfort in migrating platforms and data to the cloud vary significantly depending on the nature of the processes and data involved. A large majority (70%) of banks are already hosting their core platforms, critical processes and applications in the cloud and a further 23% expect to do so in the next three years. On the other hand, only half (50%) of banks are currently deploying cloud for non-core platforms, but a further 41% are intending to migrate these platforms, processes and applications to the cloud in the near future. This suggests that by 2028, more than 90% of platforms (both core and non-core) will be hosted in the cloud.

When it comes to data, banks are much more comfortable migrating customer data to the cloud than their own organizational data, due to the highly sensitive nature of organizational data, such as company financial and intellectual property. More than 20% of banks report that organizational data will not move to the cloud, compared to only 2% for all other processes and data.

Currently, only a quarter (27%) of banks are hosting organizational data in the cloud, a clear indication that banking leaders understand the potentially disastrous consequences of any breaches of this data. However, the research suggests this could change over the next three years, with 42% of banks planning to move some organizational data to the cloud.

Percentage of banks that plan to migrate to cloud or use a cloud service platform



1. N = 400, where N is the number of banks surveyed in Volume 5.

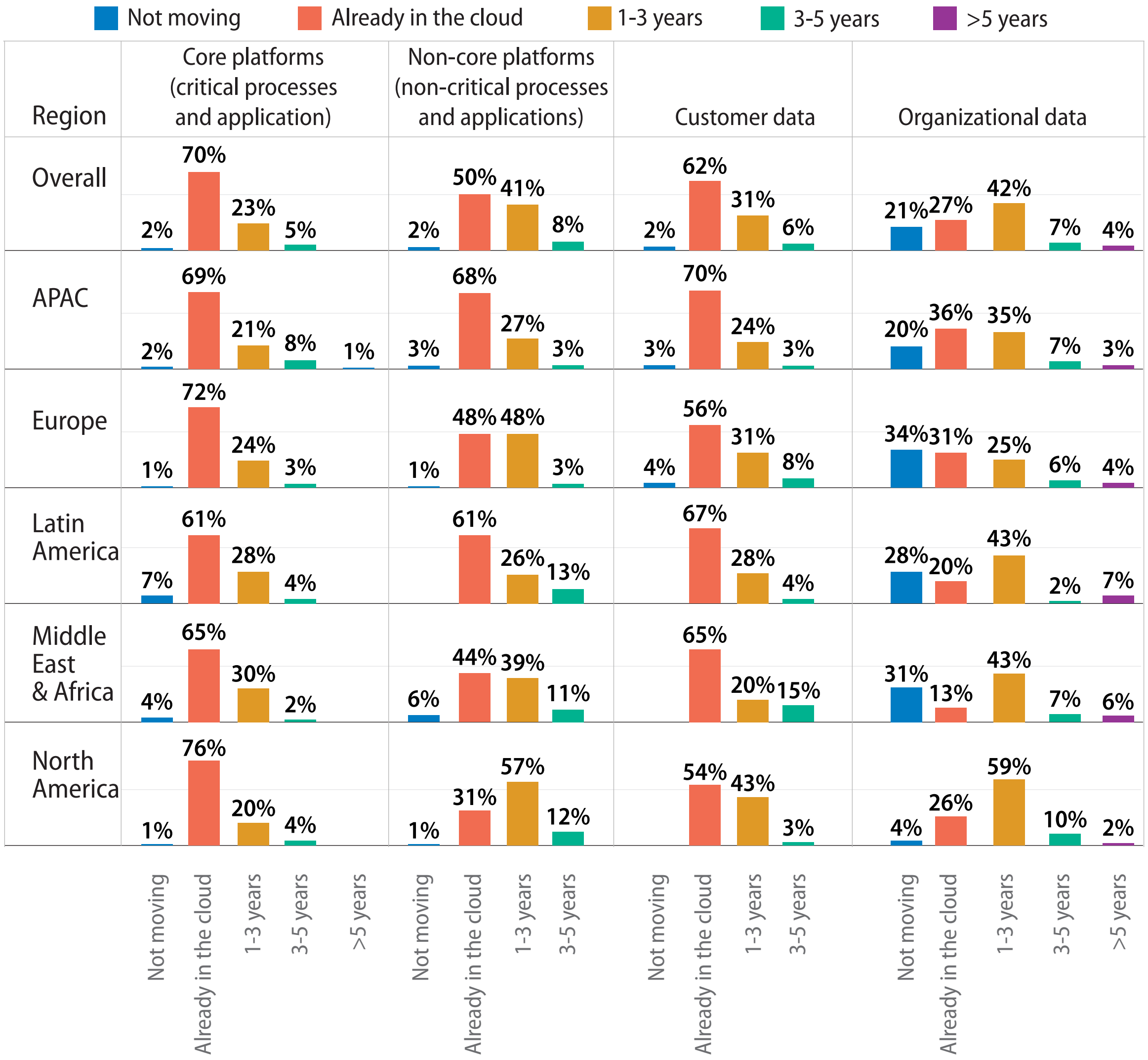
Regional variances in approaches to cloud migration

The research reveals marked differences in attitudes and approaches to cloud migration across regions.

North American banks lead the way when it comes to hosting core platforms, critical processes and applications in the cloud. 76% have already migrated their core platforms to the cloud, compared with a global average of 70%. However, when it comes to moving non-core platforms to the cloud, North American banks are lagging far behind (31% compared to a global average of 50%). Banks in APAC are leading the charge here, with 68% already hosting non-core platforms in the cloud and a further 27% planning to do so in the next three years.

Interestingly, while only a quarter (26%) of North American banks are currently hosting organizational data in the cloud (marginally below the global average of 27%), a staggering 59% plan to move organizational data to the cloud in the next three years. In line with this projected spike in cloud migration, only 4% of banks state that they will not be moving organizational data to the cloud, versus a global average of 21%. Comfort levels in relation to hosting organizational data in the cloud are lowest in EMEA.

Percentage of banks that plan to migrate to cloud or use a cloud service platform by region



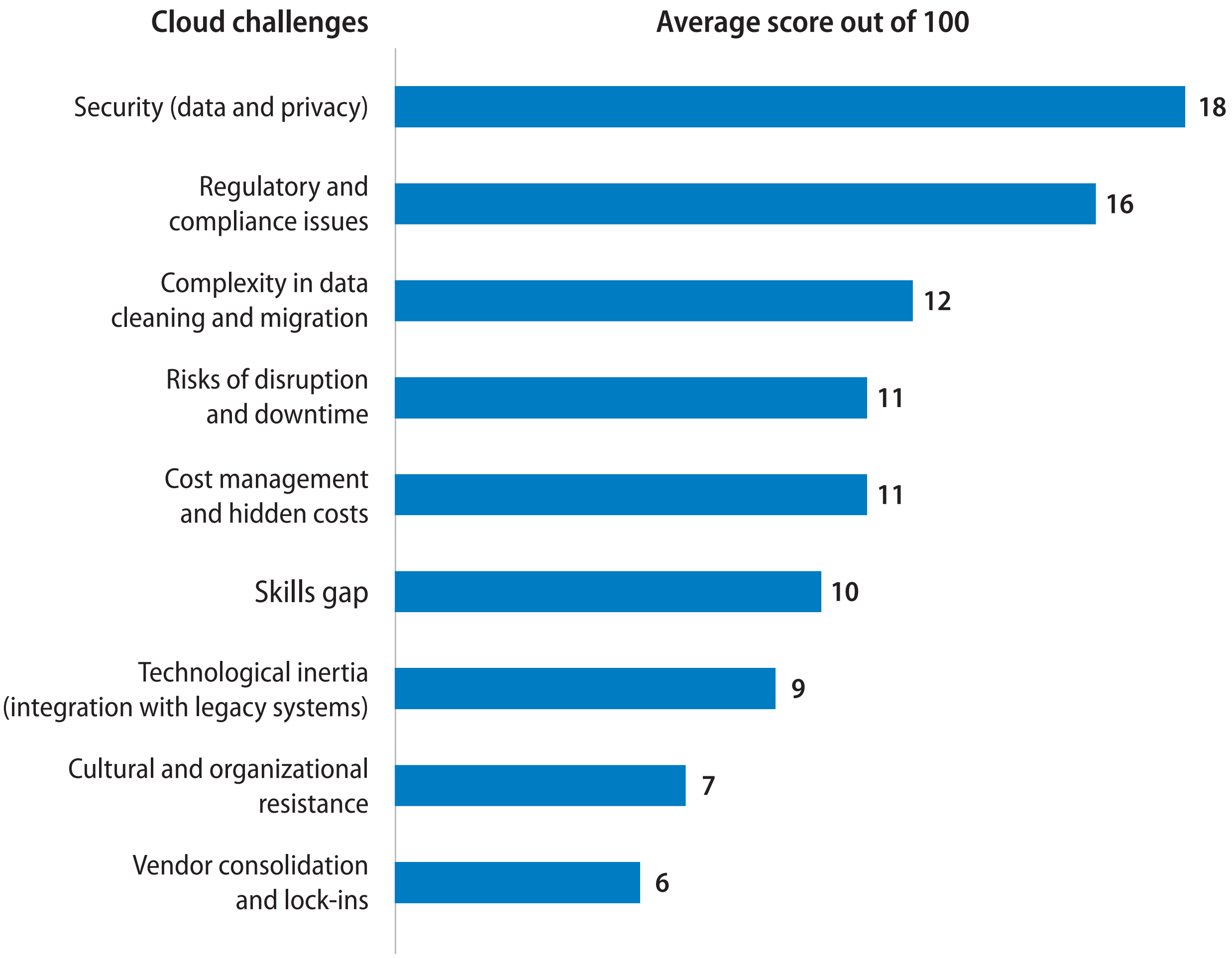
1. N = 400, where N is the number of banks surveyed in Volume 5.

The barriers to cloud migration

While sentiment towards cloud is largely positive across all regions, and many banks intend to ramp up their cloud migration initiatives over the next few years, the research identifies a number of obstacles that banks are encountering along the way. Banks point to data privacy and security, regulatory and compliance issues, and data cleaning as the top three challenges within cloud migration. With the task of handling sensitive customer data while meeting stringent compliance standards becoming ever more complex and the risks of failure so severe, security is now the most pressing concern for banking leaders.

Other barriers to success in cloud programs include cost management, avoiding disruption and downtime to applications, and accessing the necessary skills to manage large-scale migration projects. The research highlights how long-standing challenges such as the integration of legacy IT systems, cultural resistance and vendor lock-ins are still impacting some banks.

Cloud migration challenges



1. N = 400, where N is the number of banks surveyed in Volume 5.

Three steps for banks to overcome challenges and accelerate cloud migration

1. **Making data privacy and security the foundation for successful cloud migration**
   According to a survey published in June 2024, 71% of all countries worldwide have data privacy legislation in place, with a further 9% in the process of drafting new legislation. Much of the sentiment drafted within these regulations is already enshrined within GDPR as part of its 8 guiding principles. Other regulations that reference data protection add further constraints building a seemingly unfathomable weave of legislation. These regulations apply to both on-premises and public cloud implementations, but public cloud adds further complications because its ephemeral nature. Understanding this challenge is the corner stone of any cloud strategy.

A better way to tackle this conundrum is to adopt the spirit of the law. By using regulatory guiding principles to build data protection processes that address the spirit of what they try to achieve as opposed to building rules that address individual points of contention you create a more realistic approach that potentially is easier to manage. Many companies are adopting AI models in conjunction with native cloud services that predict potential compliance risks. These offer an interpretive approach that can capture a wider variety of potential risks therefore providing a more comprehensive approach that learns opposed to static fixed rule-based frameworks. Examples include predictive Machine Learning algorithms to detect future compliance risks from historical data, NLP analysis to interpret documents for discrepancies and GDPR violations, and AI chatbots for interactive, personalized compliance training.

2. Ensuring regulatory compliance on a global scale

Multinationals and other global concerns also contend with idiosyncratic local compliance issues as well as the many widely adopted regulatory regimes. For example, we have the German Bundesdatenschutzgesetz (BDSG) a federal data protection act for German federated states and in Switzerland the Federal Act on Data Protection or "FADP" which has specific provisions outside GDPR.

There are three main ways to tackle regulatory compliance on a global scale:

Consultancies and advisory firms

Many global consulting firms provide expertise to address business challenges in technology, risk, compliance, and internal auditing. These firms often use operating models that incorporate compliance within agile risk management teams. This approach enables enterprises to use analytics for predictive controls and apply regulatory knowledge when developing automated workflows aimed at improving centralized observability.

Sovereign cloud providers

New sovereign public cloud offerings- allow customers to keep data within their national borders, ensuring it stays under local laws. It also refers to how national or regional laws govern that data and how it is handled and stored within that specific jurisdiction, even when that data resides in a public cloud environment. This approach is particularly important for large financial institutions and global banks that have interests and hold sensitive information in multiple regions and are required to adhere to strict local privacy laws.

Build your own internal compliance processes to manage and oversee data security, data access and data movement.

A Data Center of Excellence is a strategic initiative within an organization, that is tasked with managing and securitizing data across all business functions and establishing a data governance framework with private data encryption and data passporting controls. Private data encryption protects information from misuse if stolen. Data passporting extends this protection to the cloud by assigning each data piece a passport that controls and can manages access across hybrid-cloud environments. Since data travels with its own encryption and passport, enterprises can secure it wherever it goes.

3. Optimizing spend and avoiding hidden costs

Cloud computing typically has a lower initial cost than traditional datacentre solutions, but ongoing cloud expenses are often underestimated as businesses service and supporting applications grow. Somethings to consider to reduce/avoid hidden costs:

- Well architected cloud native design can significantly reduce cloud spend by optimizing resource utilization and enabling automated scaling. Key strategies include adopting microservices, leveraging serverless computing, and using containerization with orchestration platforms like Kubernetes. These approaches allow for dynamic scaling based on demand, ensuring you only pay for what you use while maintaining optimal performance.

- AI and traditional automation lower cloud costs by optimizing resources, predicting needs, and automating tasks. AI agents deliver real-time analytics to adjust services based on demand, and analyse historical usage to avoid over-provisioning, reduce manual work, and make better allocation decisions, resulting in significant savings.
- The use of cloud native design, AI and other automation techniques are all key strategies within FinOps (Financial Operations) a cloud cost management practice that combines financial management with engineering and operations to reduce cloud spending. It involves implementing strategies to optimize cloud resource utilization, leverage cost-saving programs, and foster a culture of financial accountability within an organization.

There is no doubt that the evolving landscape of cloud computing and data governance demands a multifaceted approach that blends regulatory compliance, advanced technology, and cost-conscious operational models. By embracing sovereign cloud solutions, robust internal controls, and innovative strategies like data passporting, organizations can achieve enhanced data security and regulatory alignment. At the same time, leveraging AI-driven automation and cloud-native architectures empowers businesses to optimize spending and drive operational efficiency. Ultimately, success in this environment relies on fostering a culture of financial accountability and continuous innovation, ensuring that organizations remain agile, compliant, and competitive in an increasingly complex digital world.

Authors

Vijay Rathore
Infosys Financial Services, London

For more information, contact askus@infosys.com

Infosys®
Navigate your next