McKinsey
& Company

Global Banking & Securities

Fast forward: How cloud computing could transform risk management

Cloud-based computing will provide tangible benefits for banking risk management functions, but risk leaders face significant challenges migrating their systems and activities from on-premises to the cloud.

by Juan Aristi Baquero, Vijay D'Silva, Claudia Dzierbicki, and Vishnu Kamalnath

© Getty Images

September 2021

On May 11, 1997, when IBM's chess-playing supercomputer Deep Blue beat Garry Kasparov, the reigning world champion, it became apparent how computers could make judgments on par with the sharpest human minds. To process the 10^{123} possible moves in a game (far more than the 10^{82} atoms in the observable universe), Deep Blue had been programmed to proxy human judgment, using 4,000 positions and 700,000 grandmaster games. Eight years later, AlphaGo, a computer program developed by DeepMind Technologies, defeated Lee Sedol, one of the world's best players at Go, a game with as many as 10^{360} possible moves. AlphaGo used a combination of machine learning and neural network algorithms and was trained using 30 million moves. Today, AlphaZero, a successor, is considered the world's leading player of both Go and chess. It trains itself.

For years, however, this kind of computing power was difficult for most organizations to obtain. That is no longer the case, thanks to an equally dramatic change: the move from owned systems (such as the dedicated hardware of the chess and Go champions) to public cloud-based computing, giving users everywhere instant access to computing power and storage. Many businesses are embracing cloud-based software as a game changer that lets them process vast amounts of data, run new methods of advanced analytics, and benefit from more flexible technology setups. Despite rapid growth in spending (the top three cloud service providers reached $100 billion in combined revenue in 2020), cloud infrastructure still represents a small fraction of the $2.4 trillion global market for enterprise IT services.[1] A recent research effort by McKinsey Digital foresees more than $1 trillion in run-rate EBITDA (earnings before interest, taxes, depreciation, and amortization) across Fortune 500 companies in 2030 from rejuvenating existing operations, innovating in business processes, and pioneering new businesses.[2]

Despite the potential, banking has been slower than other sectors to adopt the cloud. Most banks find it difficult to give up their legacy on-premises applications, with only a few exceptions of early adopters like Capital One—which started a migration to the Amazon Web Services (AWS) cloud in 2012 and closed the last of its eight on-premises data centers in November 2020.[3]

Now attitudes are starting to change. Some in the banking regulatory community are taking a more open stance toward cloud in financial services, considering the enhanced transparency, monitoring tools, and security features of cloud computing.[4] For example, Don Anderson, chief information officer (CIO) at the Federal Reserve Bank of Boston, noted in 2019 that ignoring the cloud may even "introduce new security vulnerabilities as on-premises vendors discontinue support for their products."[5] On the other hand, regulators continue to issue guidance that highlights the key risks of cloud computing to individual institutions and to the stability of broader financial systems. In a recent report, the Bank of England noted that since the start of 2020, financial institutions have "accelerated their plans to scale up their reliance on CSPs (cloud service providers)," and that the resulting concentration among a small number of cloud providers could "pose risks to financial stability."[6] Other concerns pointed out by regulators relate to information security and the need to build cloud-appropriate risk management frameworks as an integral part of cloud migrations.

Why risk management needs to act now

Among banking activities, one of the biggest areas of opportunity for cloud computing is risk management, both for financial risks (such as credit, market, and liquidity) and nonfinancial risks (cybersecurity, fraud, financial crime). At a time when risk management leaders are being asked to process greater amounts of data in shorter amounts of time—often amid budget and staff constraints—cloud computing could unlock considerable benefits. It can help risk teams react rapidly to changes in the external environment and dive

[1] "The cloud transformation engine," McKinsey.com.
[2] Will Forrest, Mark Gu, James Kaplan, Michael Liebow, Raghav Sharma, Kate Smaje, and Steve Van Kuiken, "Cloud's trillion-dollar prize is up for grabs," *McKinsey Quarterly*, February 2021, McKinsey.com.
[3] "Capital One completes migration from data centers to AWS, becomes first US bank to announce going all in on the cloud," case study, Amazon Web Services, 2020, aws.amazon.com.
[4] Wayne Byres, "Peering into a cloudy future," speech to the 2018 Curious Thinkers Conference, September 21, 2018, Sydney, apra.gov.au.
[5] Don Anderson, "How to overcome cloud resistance in the banking industry," The Enterprisers Project, August 8, 2019, enterprisersproject.com.
[6] "Financial Stability Report - July 2021," Bank of England, July 2021, bankofengland.co.uk.

deeper into the analytics life cycle (exhibit) to better understand the drivers of risk, all without major capital expenditures.

First movers are already employing cloud-based solutions in both financial and nonfinancial risk use cases. They are, for instance, deploying them to run large and complex daily and intraday liquidity risk calculations, do close monitoring of peer-to-peer payments and mobile banking transactions, improve regulatory compliance, and get smarter about the identification of money-laundering activity. Since the pricing model for many cloud providers is flexible and usage based, cloud computing also provides economic benefits. Chief risk officers (CROs) only pay for what they use and can scale up for the surge-based computing needs of certain risk analytics activities, enabling them to shift their technology cost model from capital expense to operating expense.

By adopting cloud computing, CROs could better address four historically intractable risk management challenges: the need to process much more data, the need for more powerful processing systems, the complexity of analytics required to compete, and the greater challenges these all present to today's systems developers.

Data sets are enormous and varied

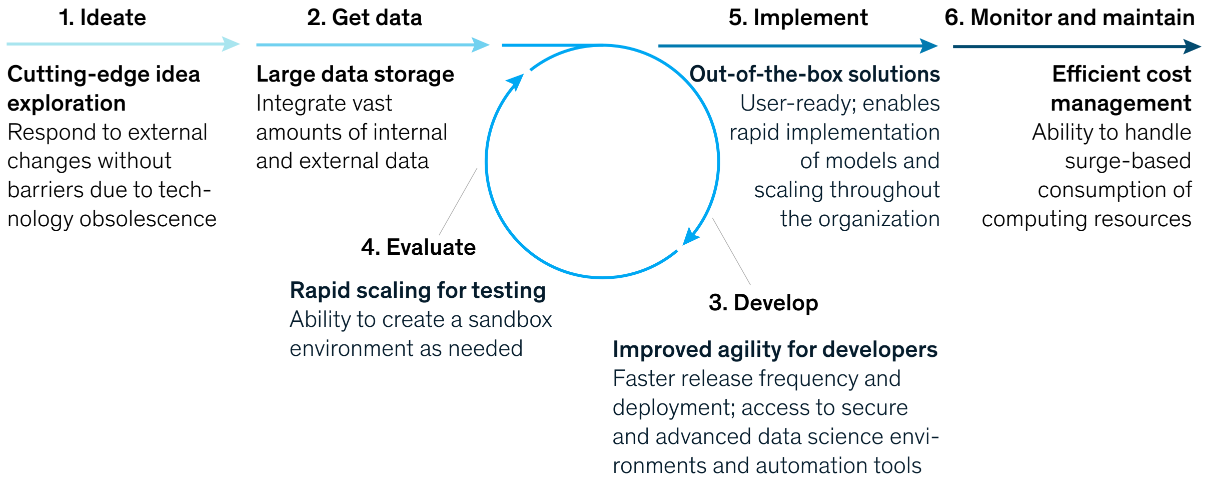
To make effective risk decisions, financial institutions have always had to convert information into insights, but today's data requirements are massive. Not only do banks gather data in greater volumes, but it comes from multiple sources and in multiple formats. For example, to assess sales conduct risk, banks are using point-of-sale transactions, sales-force performance data, consumer complaint feedback, and a range of other sources.

Developing insights from so much data is all the more difficult because financial institutions often house their information in disconnected systems and then govern these systems through different processes. This siloed approach makes it hard to integrate internal and external sources of information and develop a complete and unified view of risks. As a result, teams can miss useful insights.

With cloud-based solutions, risk management teams have the potential to easily and quickly

Exhibit

Selected benefits across the six stages of the life cycle for risk model development.



1. Ideate

Cutting-edge idea exploration
Respond to external changes without barriers due to technology obsolescence

2. Get data

Large data storage
Integrate vast amounts of internal and external data

3. Develop

Improved agility for developers
Faster release frequency and deployment; access to secure and advanced data science environments and automation tools

4. Evaluate

Rapid scaling for testing
Ability to create a sandbox environment as needed

5. Implement

Out-of-the-box solutions
User-ready; enables rapid implementation of models and scaling throughout the organization

6. Monitor and maintain

Efficient cost management
Ability to handle surge-based consumption of computing resources

Source: McKinsey analysis

integrate many different data sources and systems. Some solutions have standardized, easy-to-use web-based interfaces, which eliminate the need for specialized configurations between a bank's systems and those of a third party. American Express, for instance, introduced its cloud-based Cornerstone data ecosystem several years ago to share capabilities and data across functions and geographies.[7]

Data volume and analytic tasks require tremendous computing power

Processing the large data sets needed for sophisticated advanced analytics and machine-learning models requires heavy loads of computing power, especially when multiple legacy systems are involved. Banking risk management functions seldom have access to such high levels of computing power, and resource barriers prevent teams from simply adding more servers.

Cloud deployments offer a more flexible model, pioneered by AWS elastic-computing capabilities, giving teams access to on-demand increases in computing power and a library of easy-to-deploy tools. Today those capabilities are changing the way banking's risk function operates. One leading bank was able to multiply the processing power dedicated to the Monte Carlo simulations it uses for trading risk projections, running them in a matter of hours as opposed to multiple days, according to executives at Microsoft Azure. At one investment bank, the relaxation of legacy computing capacity constraints enabled by cloud computing resulted in a significant increase in the use of analytics: more experimentation by trading strategy teams and adoption of new types of analyses they could not have tried before (e.g., modeling certain types of interest rate volatility directly rather than assuming it).

Similarly, a global systemically important bank had been assessing global liquidity by running its model 14 hours a day. After the bank switched to a cloud-based solution, the time dropped to less than three hours, allowing risk teams to do more frequent analyses and iterations, incorporate additional data, and make quicker business and balance sheet strategy decisions, according to executives at Google Cloud.

Migrating to a cloud-enabled platform can also streamline upgrades. Instead of spending substantial time and effort configuring new upgrades and capabilities on disconnected legacy systems, risk teams let their technology partners handle both the software and hardware upgrades. This reduces ongoing technology operating costs and minimizes the risk of obsolescence in an age of rapid evolution.

The bar has been set high for data analytics

In recent years, cloud-based providers of risk management solutions have developed a wide variety of innovative, user-friendly, out-of-the-box automation tools, such as data drift analysis, critical misconfiguration alerts, and digital forensics tools. Utilizing such technology frees up risk analysts' time to focus on what they do best. Instead of spending time configuring tools and technology, they can move quickly to develop sophisticated models and alert mechanisms. Barclays freed up time for its risk analysts by working with a cloud-based provider to improve its automation process for granting transaction risk analysis exemptions for merchants.[8]

Executing risk management in the cloud also makes it easier for teams to recalibrate and manage their models and set up new tests. Cloud-based infrastructure can be continuously fed with real-time data—something beyond the capabilities of many legacy systems. This makes models more accurate and precise, and helps analysts quickly make data-based decisions on their effectiveness.

HSBC, for instance, uses cloud computing services to look for money-laundering and other criminal activity in a completely new way. By mapping networks of connections between people and companies, the bank's Global Social Network Analytics platform lets risk management teams

[7] Randy Bean, "How American Express excels as a data-driven culture," *Forbes*, March 15, 2018, forbes.com.
[8] Louis Columbus, "How Barclays is preventing fraud with AI," *Forbes*, June 11, 2020, forbes.com.
[9] Trond Vagen, "HSBC set to launch cloud-based AML system next year, says senior official," Reuters, November 28, 2018, reuters.com; Gary Flood, "HSBC – using AI to join the financial crime 'dots,'" Diginomica, January 28, 2021, diginomica.com.

find suspicious transactions that previously were identifiable only by humans.[9] Using cloud services, another bank detected a data breach and found the individual responsible within two weeks, while at a competitor, the detection and apprehension of the same breach took over a year, according to executives at Google Cloud.

Systems developers need the agility of cloud computing

The flexibility and connectivity of cloud-based environments can have a meaningful impact not only on the productivity of risk analysts but also on the developers who create and maintain the models that identify, measure, and mitigate risks. After moving to the cloud, developers often report significant improvement in key performance metrics, including improvements in release frequency, lead time to deploy, and mean time to recover. Commerzbank, for instance, says its developers use cloud services to follow a continuous integration and delivery (CICD) approach, enabling them to do code updates much more seamlessly and easily.[10]

Finally, the impact of cloud-based solutions extends beyond the risk function, since their ease of use makes robust risk identification and assessment tools more accessible to business units, which are the first line of defense. This allows for a better understanding of risks and a sense of ownership for risk decisions. Loan officers, for instance, can stress test loan portfolios or simulate the performance of a loan before approving it, enabling a deeper awareness of risk-return trade-offs.

Managing the transition

While the potential benefits of cloud computing are substantial, so are the challenges of migrating risk management systems and activities from on premises to the cloud. CROs must plan for managing complexity, investing the necessary resources, and meeting needs for new capabilities and culture.

For the most part, risk systems are not stand-alone; they thread through the bank's core applications and processes. As a result, moving risk applications to the cloud may have implications for other systems and ultimately require the reconfiguration of other applications. Thus, the migration journey for risk applications needs to be designed as part of the broader enterprise migration, which will involve hundreds of applications in total. Some companies have established a private cloud in which computing resources are hosted on a network used by only one organization and located within their own data center. Others have opted for a hybrid between this approach and the public cloud hosted by a major provider.

Migrating to the cloud can have a significant impact on financial statements. Although the legacy technology systems on which banks often operate carry maintenance costs, their depreciation expenses are minimal. While most cloud providers offer incentives for multiyear commitments that can offset near-term migration costs, substantial expenses will still hit the P&L. Therefore, investments needed for cloud migration and the subsequent operating costs must be carefully planned and sequenced over time to manage their financial impact.

The skills required to migrate and operate in the cloud include a much heavier focus on engineering and data science than is needed for on-premises computing. This kind of talent is difficult to recruit and even harder to retain, especially amid currently high attrition rates. In addition, the culture of teams working in the cloud is faster moving, more adaptable, and more focused on rapid delivery. Risk functions at banks will need to adjust their operating model to enable this new culture while keeping the rigor, control, and governance required for risk management activities.

[10] Google Cloud, “Commerzbank and Google Cloud strengthen strategic partnership,” press release, March 29, 2021, cloud.google.com.

What CROs and risk leaders can do

Given these challenges, migrating to the cloud isn't an express trip. Instead, for most risk leaders, it is a multistage journey that will need planning and execution within the broader cloud strategy of the entire organization. As our colleagues have pointed out recently,[11] companies that adopt cloud have to manage their overall strategy and business case, adoption in each business domain, and the construction of foundational capabilities that enable security and scale, all in concert.

CROs and other risk leaders have an important role driving adoption across the risk domain, but also can influence the overall strategy and business case, and need to help scope the foundational capabilities required, in particular when it comes to security and controls. Three actions can help guide the cloud adoption journey for risk management:

1. *Set a holistic aspiration for adoption.* As banks compete with cloud-based fintechs and other attackers, their ability to manage risk should be one of their biggest advantages. Yet the number of risk management apps that have to be migrated can be daunting. A forward-looking cloud strategy will need to be in line with the ambitions and pace of the company's overall cloud transformation, especially given the complex ways in which risk technology systems are intertwined with those of the broader organization. Picturing the endgame of what data sets make it to the cloud and how the data will be used could serve as a North Star.

2. *Develop multiple waves of use cases in priority risk domains.* Along each step of the migration journey, risk leaders must figure out which models or functions to migrate to the cloud first. Choosing the right use cases among a mind-numbing quantity of possible options combines risk leaders' input on the potential benefits with technology leaders' feasibility and cost-benefit analysis. Ultimately, the tasks most suited to cloud adoption are those that require heavy computation, speed, and extensive integration of external data with third parties.

   The common error of scattering tests and use cases throughout multiple domains will not create the momentum delivered by a deep dive into one or two major domains, whether consumer credit risk, trading risk, or consumer fraud. This is because the migration of data and tech to a cloud provider is often the toughest challenge. Once a single use case is complete for a given domain, it's easier to develop additional use cases in parallel.

3. *Rethink the operating model, skills, and culture needed for effectively managing risk in the cloud.* As frontline business teams take greater ownership of risk decisions and more monitoring tasks are automated, the activities, talent, and skill requirements of risk teams will change. The risk function will need a larger proportion of analytical and technical talent to develop, maintain, test, and continuously improve risk models and tools in the cloud. Risk leaders should evaluate how this will transform the way the risk function operates.

A transition to cloud-based risk management offers too many benefits for risk leaders to ignore. For banks, cloud computing is quickly becoming an imperative. Those that do not migrate their systems and capabilities could lose the ability to innovate quickly and respond effectively to the competitive pressures and increasing number of risks facing banks. The many decisions to make along the journey can paralyze firms, but a focus on the key issues and a prudent approach to implementation can help risk managers think several moves ahead on the chessboard.

Juan Aristi Baquero is a partner in McKinsey's New York office, where **Vijay D'Silva** is a senior partner; **Claudia Dzierbicki** is a consultant in the Toronto office; and **Vishnu Kamalnath** is an associate partner in the Boston office.

[11] "The cloud transformation engine," McKinsey.com.