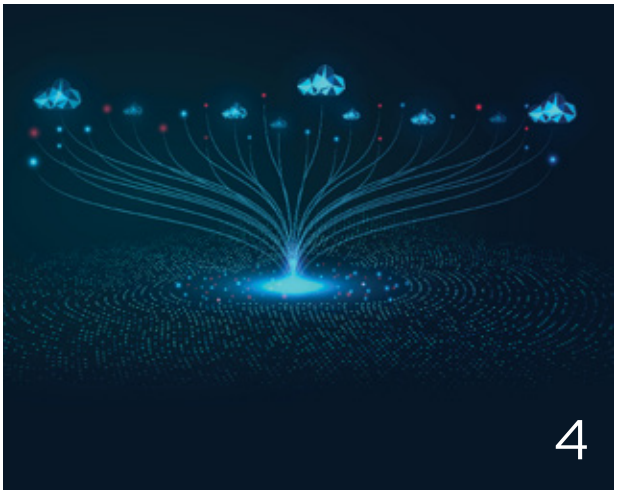
CENTRAL BANKING AND CLOUD SERVICES: THE NEW FRONTIER

DMI OMFIF Digital Monetary Institute

CONTENTS



CENTRAL BANKING AND CLOUD SERVICES: THE NEW FRONTIER

FOREWORD

UNLOCKING THE POWER OF PUBLIC CLOUD

Regulations are evolving and institutions are recognising the need to address operational resilience. By Howard Boville, senior vice president and head of IBM Cloud Platform & Technology Lifecycle Services.

EARLY in 2023, the US Treasury released its cloud report, highlighting considerations for financial services organisations when working with a cloud provider. Moves like this indicate that US policy-makers and regulators are following the lead of their UK and European counterparts in intensifying oversight of public cloud usage, scrutinising the risk posed by engaging with third- and fourth-party vendors and focusing on the need to mitigate concentration risk coming from cloud service providers.

The regulatory scale is tipping from a focus on IT risk management to a broader consideration of the operational and digital resilience needed for financial stability and service dependability. The goal is clear: to minimise the impact of disruption and the risk of customer harm by closing gaps in the supply chain. IBM believes that security, reliability and trust need to be at the centre of decision-making on where enterprise workloads and applications reside.

While central banks have a very different mission to commercial financial entities, what they have in common is the need to modernise their IT operations to support the digital transformation and analytical use cases, contain costs, source key skills and mitigate operational and cybersecurity risks.

Central banks have a complex relationship with public cloud technology: they are some of the most sophisticated users in financial services with analytical demands of immense scale, complexity and criticality. They are also increasingly positioned as prudential overseers of public cloud usage and cloud service providers themselves. While the duality may create tension, this two-pronged posture is important because the learning-by-doing on the IT side of central banks can provide invaluable insight into the opportunities and challenges that public cloud technologies bring to the sector.

Done correctly, I believe cloud can deliver unparalleled benefits in performance and total cost of ownership without compromising resiliency, security and compliance. But delivering on this vision requires a concerted effort across the entire financial services ecosystem. Without an approach that balances the ambitions of individual firms with collective, societal responsibility, the promise of cloud technology risks getting lost amid regulatory uncertainty and technical fragmentation. This is why I am such a strong advocate of initiatives that bring us together as a community to drive better outcomes.

One of the aspects I am most encouraged by is how the entire financial services industry, from large global institutions to regional and community banks, is coming together to learn and share best practices and ideas. Over the last five years, we have been working with global and regional financial institutions to de-risk cloud consumption. With the IBM Financial Services Cloud Council – a trusted network of more than 130 financial services experts – and our continuous dialogue with regulators and likeminded organisations such as the Cloud Security Alliance, we are harnessing the intelligence of the industry. As a result, we have built a consistent standard for security controls that addresses the evolving regulatory and threat landscape through the IBM Financial Services Cloud Framework.

I see public cloud as an enabler of a better future for financial services, not as a destination. For every stakeholder in the ecosystem, evolving operational resilience and third-party regulation is a reminder that the industry needs broad collaboration incentivised by outcome-orientated policies that enables cloud-native innovation and safeguards financial stability. Working together intelligently, I firmly believe we can ensure that one set of desirable outcomes does not come at the cost of the other. ■

> “
>
> DONE CORRECTLY, I BELIEVE CLOUD CAN DELIVER UNPARALLELED BENEFITS IN PERFORMANCE AND TOTAL COST OF OWNERSHIP WITHOUT COMPROMISING RESILIENCY, SECURITY AND COMPLIANCE.

INTRODUCTION

CLOUD: THE NEW FRONTIER

Central banks are increasingly turning to new technologies and strategies to manage their expanding responsibilities and requirements for data collection, storage and analysis.

USE of the public cloud is fast becoming ubiquitous in financial services. A survey conducted by the American Bankers' Association in 2021 found that more than 90% of institutions in the US banking industry are using the cloud for some of their applications.

Many third-party providers are discontinuing their on-premises product offerings and providing applications and services only within cloud infrastructure. While individual central banks, along with the Bank for International Settlements and the Financial Stability Board, have voiced concerns about the dependence of the financial sector on cloud service providers and the potential impact on financial stability, the need for sophisticated data analysis software means that it is becoming increasingly difficult for them to avoid cloud entirely.

The ability to pass off responsibility for managing data centre infrastructure to a third party with the potential to benefit from on-demand self-service, resource pooling, scalability and rapid elasticity, pay-as-you-go pricing, reliability, availability and security has proven a compelling argument for many private sector financial institutions to migrate parts of their infrastructure to the cloud. Central banks are increasingly receptive to the benefits of the public cloud model and can learn from and build on the experiences of commercial banks that have already advanced their cloud adoption.

At least in the short term, certain private sector financial institutions are opting for a hybrid approach, keeping the most sensitive data – personally identifiable information – in on-premises storage, while benefitting from the superior technology available from cloud service providers for less sensitive data. As comfort around encryption capabilities grows, however, organisations are likely to be happy to migrate more sensitive data to public clouds as well, to the extent permitted by regulation.

However, central banks are reluctant to relinquish the control over their data that an on-premises architecture gives them. This is despite the fact that they have many of the same needs as private sector enterprises, as well as the same responsibilities to keep their data and infrastructure safe from cyberattack or ordered release.

For commercial banks, the move to cloud has provided advantages that central banks are denying themselves because of their preference for managing their own on-premises infrastructure. For this report, we conducted interviews with central banks and private, regulated financial infrastructure providers on their cloud strategies, building up a picture of what cloud can offer central banks and the challenges they face in adopting it.

As well as exploring the benefits that cloud migration offers central banks, we examine the ways in which financial institutions in the private sector have addressed the hurdles that are hampering central bank cloud adoption. Some of these challenges are technical, some are legal, while others are cultural, and different solutions are needed to address each.

We hope that this paper will help to shed light on the remaining obstacles, highlight possible solutions and provide impetus for further ecosystem-level collaboration between policy-makers, banking supervisors, financial institutions, cloud service providers and IT and cloud practitioners from all stakeholder groups. ■

KEY FINDINGS

Regulatory challenges are a major obstacle in many jurisdictions but ensuring that regulators are well-educated about the benefits of technology and the risk-mitigating safety features that are available can help.

Public cloud infrastructure benefits from economies of scale that do not apply for single-tenant architecture. These benefits include:

- Users get much quicker access to premium technology than would be economically feasible for an on-premises set-up.
- Users get access to computational resources on a pay-as-you-go basis, rather than having to purchase resources for their peak needs.
- Users benefit from a cybersecurity threat response team that is available 24/7 without needing to invest directly in these resources themselves.

Data sovereignty is among central banks' biggest concerns around cloud migration. However, many other regulated entities, including banks and other financial market players, are effectively mitigating the sovereignty risk with a combination of legal and technical tools. These include:

- Hybrid cloud architecture to keep sensitive data on premises
- Legal guarantees of data localisation
- Cryptographic 'keep-your-own-key' security measures

CHAPTER 1

EMBRACING THE CLOUD

While there are some concerns preventing central banks and institutions from fully adopting cloud technology, there are also clear benefits to doing so.

ADOPTING cloud technology can enable users to access cutting-edge capabilities and simplify their IT operations. Although it can be a challenging transition to manage and requires complex redesigns of systems, consensus is building that this work is worth the effort.

Regulatory barriers

The first and most obvious obstacle to embracing cloud technology is that the decision to migrate to public cloud infrastructure does not always sit with the central bank. Many governments formulate policies that limit the ability of public institutions to use public cloud infrastructure. Some allow this use but only if the data centres are in the same country or within the same region (European Union governments typically require public institutions to store data within the EU and with providers that are headquartered there). Others only allow the use of certain providers, often those headquartered in the country.

The Bank of Korea, for example, only allows public institutions to use cloud services that are qualified by the Cloud Security Assurance Programme. Thus far, this list includes only domestic cloud service providers, but it is likely that their global counterparts will join them soon.

In Europe, national central banks will have to pay close attention to the guidelines agreed by the European System of Central Banks' IT committee, on which all the constituent central banks are represented. 'Once the guidelines from the ESCB are published, we will have to factor that into our own IT strategy,' said an official from a central bank who asked to remain anonymous.

The absence of regulatory clarity remains a major stumbling block for broader adoption in financial services, both for the public and the private sector. In a report published in December 2022, the Association for Financial Markets in Europe cited regulatory complexity as one of the major challenges slowing cloud adoption. This conclusion has been echoed in research in other jurisdictions. This is particularly the case for Europe, where localised implementations of bloc-wide regulations have complicated the landscape.

It is likely that this consideration affects public sector institutions more severely than those in the private sector. Where the private sector can seek legal advice and make the best effort to comply with regulations as they understand them, public institutions tend to be even warier because of reputational risk.

Overcoming these regulatory hurdles is an important challenge. It is only through liaison with their government that central banks might be able to effect changes in the regulation that gives them the freedom to decide to use public cloud. These discussions must be framed by a clear understanding of central banks' data infrastructure needs, the problems they face and the solutions cloud providers can offer.

> "THREE YEARS AGO, I WOULD HAVE SAID WE ARE NOT GOING TO MIGRATE TO PUBLIC CLOUD INFRASTRUCTURE BECAUSE WE CAN'T BE CONFIDENT IN THE CYBERSECURITY OF CLOUD SOLUTIONS. BUT THE PANDEMIC PUSHED US TO IT.
>
> **Central banker who asked to remain anonymous**

Flexible access to large-scale computational power

One of the core value propositions of cloud services is the flexible access to large-scale computational power. This consideration varies in importance depending on the activities of the central bank.

For central banks that directly or indirectly manage payments systems (whether retail like the Banco Do Brasil's Pix, or wholesale like the Saudi Arabia Monetary Authority's sarie), high computation capacity is a key consideration.

While it is possible to build sufficient capacity even for high-volume trading platforms on premises, load variability makes this challenging. 'With the demands entailed by transaction peaks, it's important to have cloud. Without the load balancing cloud offers, less sophisticated systems can be overwhelmed,' said Majid Malaika, chief adviser to the SAMA vice governor and an expert on cloud computing and cybersecurity. 'Yes, it's possible to replicate that environment with on-premises architecture, but that means building enough capacity to support peak volume.'

Consider the difference between the capacity required at 4.30pm on the last shopping day before Christmas and 12 hours later. For much of the time, it is likely that only a tiny fraction of the peak computational power will be required.

Cloud services allow computational power to be delivered flexibly, as needed. For central banks considering a central bank digital currency, this is likely to be an important factor. While developing the capacity in-house is certainly possible, it is much more difficult than using a cloud services provider.

But even central banks without payments systems to manage might have a need for large-scale computational power. Artificial intelligence and machine learning are increasingly common tools for central banks to perform analysis of large volumes of data, particularly when that data is in an unstructured format.

'We are experimenting with high-performance machine learning,' said Bruno, head of IT, economics and statistics, Banca d'Italia. 'We are using public cloud environments to train neural networks or machine learning models. In our experience, by using public cloud infrastructure we can reduce training time substantially relative to conducting the same work on premises.'

As with payments systems, demand for this kind of computing power among central banks is often likely to be an occasional necessity. 'It makes sense for us to use that capacity on a pay-as-you-go basis,' said Bruno. 'For us to buy hardware that gives us that kind of capacity would be expensive, particularly when we don't need it every day.'

Access to premium technology

Software as a service is an increasingly prevalent delivery model. Central banks are fast discovering that some level of comfort with cloud-hosted services is likely to be necessary if they are to operate at the level of efficiency they expect.

The Covid-19 pandemic has catalysed a significant change of attitudes among many central banks on this point. 'Three years ago, I would have said we are not going to migrate to public cloud infrastructure because we can't be confident in the cybersecurity of cloud solutions,' said a central banker who asked to remain anonymous. 'But the pandemic pushed us to it. We had an outdated conferencing tool when the pandemic hit and high-level management within the bank demanded that we get access to a more sophisticated collaboration tool.'

'Taking that decision required us to assume additional risk, but it enabled us to discover that we can do things in the public cloud safely and securely,' they said. 'The team was tasked with making our collaboration tools secure in the public cloud and they achieved it.'

While this is a relatively modest step compared to those taken in the private sector, it reflects an important development: becoming comfortable with operating SaaS in a secure fashion opens the door to more elaborate cloud integration.

The flexibility public cloud services offer also gives customers access to the newest and highest-quality equipment. This is an important consideration for both central banks and private customers.

'For us, the most significant consideration for cloud adoption is the access to newer technological stacks. It's not feasible for us to bring in new functionalities on premises as quickly as cloud providers can do it,' said Andrzej Mikolajczak, group chief technology officer at Euroclear.

The economies of scale that cloud service providers can leverage make it far more feasible for them to deliver the most sophisticated and modern equipment on a constantly updated basis in comparison to on-premises infrastructure. The scale and variety of public cloud customers' needs mean that it is economically efficient for them to provide top-end equipment almost as soon as it becomes available.

This is, generally speaking, impossible to achieve with on-premises infrastructure. Bruno explained: 'Typically, our IT equipment has a lifecycle of around five years, which allows us to amortise the costs over the period. A lot of our infrastructure will be in place for a substantial time.'

Using a cloud services provider is not necessarily a cost-saving measure here. In Bruno's experience, the prices for the major cloud services provider were not substantially cheaper than the cost of purchasing the equipment, amortised over its lifespan. However, even if the costs are the same, using public cloud infrastructure means that, over a period of five years, the customer is using constantly updated technology, with improved performance or security standards.

In the case of on-premises infrastructure, as well as the cost of purchasing new hardware and software, central banks must retain the expertise necessary to install and maintain that equipment in-house, which can prove challenging.

Easing staffing challenges

A major consideration behind the private sector's migration to public cloud infrastructure is the fact that it reduces the scale and complexity of resources they need to find and dedicate to building and maintaining their data infrastructure.

Staffing in this area is particularly difficult. Many in the financial services and central banking community have found it difficult to find staff that have the skills and expertise required to build and maintain their own infrastructure.

This is a particularly important consideration for smaller central banks, where resources are more limited. Many infrastructure maintenance issues, and

> "THE USE OF PUBLIC CLOUD SERVICES CAN BE DONE WELL IF THE INFRASTRUCTURE IS DESIGNED AND SET UP CORRECTLY. BUT THE PEOPLE WHO HAVE THE EXPERTISE TO SET UP INFRASTRUCTURE OF THAT COMPLEXITY ARE STILL RARE.
>
> **Dirk Thomas, Big Data Advanced Analytics, Commerzbank**

especially cybersecurity services, require teams to be available to respond to threats 24/7.

It is also important to acknowledge that central banks with more complex needs will require more complicated infrastructure. Building a payments infrastructure in the public cloud is a particularly complex undertaking. 'The use of public cloud services can be done well if the infrastructure is designed and set up correctly,' said Dirk Thomas, who works on big data advanced analytics at Commerzbank and built up the European Cloud User Coalition. 'But the people who have the expertise to set up infrastructure of that complexity are still rare.'

The marketplace for data technology professionals is extremely hot and public institutions often find it difficult to compete with the salaries and flexible working arrangements offered by the private sector. Cloud services allow much of this responsibility to be outsourced. Cloud service providers can easily supply the technical expertise required to procure, install and maintain data centre hardware and software.

However, for central banks to be comfortable with the data centre management strategy being conducted by a third party, it might require them to conduct tours to review the controls. This was particularly difficult to arrange during the Covid-19 pandemic.

Disaster recovery and operational resilience

One of the advantages that led to commercial banks embracing cloud technology is the ease with which cloud services can provide facilities for disaster recovery. On-premises solutions require remote data centres to ensure service continuity in the case of accidents or a natural disaster rendering the main centre unusable. These can be expensive and complicated to develop and maintain.

The cloud can store copies of customers' architecture in multiple locations simultaneously, allowing customers to switch from their primary data centre to a redundancy option with little or no loss of data. Though cloud services can be expensive, the complexity of building and maintaining disaster recovery services can at least partly be outsourced to the cloud provider.

However, many central banks envisage a situation where only part of their infrastructure is migrated to the cloud. Some data, particularly any personally identifiable information, will most likely remain on premises for the foreseeable future. This means they will still have disaster recovery components to manage themselves, but the requirements may be less onerous if a substantial part of their infrastructure is in the cloud.

It is important to remember that, though reliable, public cloud infrastructure is not infallible. Cloud migration brings its own challenges from a disaster recovery perspective. The simplest approach to cloud adoption is to use a single provider for all cloud-based applications. This reduces the complexity of training and development required and makes threat monitoring simpler.

> "THE MARKETPLACE FOR DATA TECHNOLOGY PROFESSIONALS IS EXTREMELY HOT AND PUBLIC INSTITUTIONS OFTEN FIND IT DIFFICULT TO COMPETE WITH THE SALARIES AND FLEXIBLE WORKING ARRANGEMENTS OFFERED BY THE PRIVATE SECTOR. CLOUD SERVICES ALLOW MUCH OF THIS RESPONSIBILITY TO BE OUTSOURCED.

However, this approach carries risks. Some users may wish to avoid being locked into the services of a single vendor. Central banks must consider the possibility that the cloud provider they select, rather than an individual data centre, might become compromised in some respect, perhaps from a cybersecurity or data sovereignty perspective.

In such a case, central banks must be able to quickly migrate their infrastructure either to another non-compromised cloud provider or to their on-premises infrastructure, without substantial disruption to their service. This kind of flexibility will require them to develop a hybrid approach (combining public cloud with on-premises infrastructure) or a multi-cloud approach. If the exit strategy requires applications to be brought on premises, the user's infrastructure must have sufficient capacity to support this. Otherwise, the customer must have a working relationship with multiple cloud service providers. Switching applications from one cloud to another is not a simple task and involves additional operational complexity.

Euroclear, a central securities depository, has been working with its main regulator, the National Bank of Belgium, to develop a cloud policy. Mikolajczak said: 'We built and are strengthening our cloud policy in a close collaboration with the regulator. Developing an exit strategy for if a cloud provider is at continuity risk was among their main concerns. In the long term, with a multi-cloud approach, we might be able to move between clouds. In the short term, we will work on an application-by-application basis. Some would likely be ported to other clouds, while some would be brought on premises as part of our hybrid approach.'

So, while cloud offers a valuable solution for efficiently storing data in a resilient fashion, central banks and other institutions will most likely maintain on-premises infrastructure, if only as a fall-back in case of a cloud provider becoming compromised. ■

CHAPTER 2

RISKS AND TRADE-OFFS

Adopting the cloud comes with challenges and creates security risks, which are deterring some institutions from fully making the transition.

Cybersecurity

THERE is a trade-off inherent in the decision to move to the public cloud. Banca d'Italia's Bruno explained: 'From one standpoint, the cybersecurity infrastructure by major cloud providers is even more secure and reliable than what you find inside central banks. However, the exposure they face is so much higher than on-premises infrastructure.'

Nevertheless, the consensus among interviewees was that major providers of global scale are all able to provide extremely good cybersecurity. Mikolajczak from Euroclear said: 'In certain aspects, cloud can provide even better security partly because the speed of innovation among cloud providers is greater than we can timely manage.' He added that, even though Euroclear's critical systems are managed on premises, some of its cybersecurity features come from its cloud provider.

Cloud providers have a number of advantages in the cybersecurity arena. First, the ability to provide top-quality hardware and software quickly means that they are not relying on dated and potentially vulnerable equipment. Second, their economies of scale mean that they can provide 24/7 threat monitoring and response services that many customers will struggle to match. Third, while their infrastructures are more exposed to threat, the ability to share information globally means that they are often better prepared against new threats than on-premises security infrastructures.

It is worth acknowledging that cloud providers are not all equal in their ability to offer protection from cyberthreat. 'The major providers have very impressive capacity to deal with a variety of cyberthreats,' said Malaika from SAMA. 'The mature cloud providers are significantly ahead of smaller, newer, local competitors. Often, analysis of those shows vulnerabilities.' Thomas at Commerzbank agreed: 'The deep dives into the security solutions of some providers may reveal serious deficiencies.'

However, even having selected a cloud provider with a sterling reputation for robust cybersecurity, the implementation is not straightforward. 'The truth is that, even having selected a provider with great cybersecurity infrastructure, security is an end-to-end consideration. If the customer has weak development or change management processes, it is possible to exacerbate risks,' Thomas said.

> LUXEMBOURG SIGNED AN AGREEMENT WITH ESTONIA, GRANTING THE DATA ESTONIA STORES IN DATA CENTRES IN LUXEMBOURG THE SAME LEVEL OF INVIOLABILITY AND IMMUNITY AS PHYSICAL EMBASSY BUILDINGS.

To ensure that central banks have access to the best cybersecurity and threat response systems available, it seems they must be able to use global cloud services providers. However, a rigorous, security-focused change management service will need to be in place to ensure that cloud migration delivers security benefits.

Data sovereignty

Perhaps the most uniformly held opinion on cloud in central banking IT departments is that migrating to cloud poses a major risk to their ability to keep data private. Although some are coming around to the idea that properly designed cloud architecture can provide adequate cybersecurity, this is no defence against the possibility of a foreign country simply asking the cloud services provider to reveal its customers' data.

'They are right to be concerned,' said Malaika, who focuses on cybersecurity at SAMA. 'I've had many conversations with cloud providers, where they admit that, if they are asked to reveal customer data hosted in their cloud, by law, they will have to comply and they will not necessarily inform their customers that they have done so.'

Others believe that this concern is overblown. Thomas said that, although technically accurate, the concern was misplaced. 'I see the risk of US security services taking data from data centres is overrated. If they need data from banks to fight financial crime, for example, they don't order the cloud provider to release it. They are more likely to ask for legal aid and contact the relevant authorities or us directly. To me, the threat of ordered release is unlikely to happen.'

If central banks are to become comfortable with public cloud infrastructure, addressing this concern is paramount.

Mitigating the sovereignty risk

The first means of addressing this issue of data sovereignty is to ensure that the central bank data remains on servers based in the bank's country. This can happen in a number of ways.

First, banks can use a locally based cloud provider. This can be an attractive option for state actors because, as well as keeping their data in country, it allows them to support a local business. However, both Malaika and Thomas agreed that going with a smaller cloud service providers may mean making compromises on cybersecurity and services. Thomas pointed out that, if central banks are forced to compromise on securing data against ordered release by the US government or cyberattack by actors in Russia, China or North Korea, the latter is an obviously more damaging risk.

Local providers may not be able to offer the full range of sophisticated services that large cloud providers can. Major cloud providers can offer a software layer built within a local provider's data infrastructure, ensuring customers have access to their services. This 'satellite' approach addresses some deficits but the hardware layer is owned and operated by a local provider, which can create vulnerabilities.

Cloud providers can also offer legal assurances that their customer data will remain in country (or within the EU, which is a common requirement for European customers). However, as this kind of requirement becomes more widespread, it will be challenging for cloud providers to maintain the same security level and the resilience of their services. One of the challenges is that regulators and customers do not always engage with the question with the appropriate degree of nuance. This can result in them not distinguishing between the data customers wish to store in the cloud and metadata about the customers' usage.

While some of this metadata might be sensitive and should be protected, some of it is likely to be innocuous but nevertheless important for cloud providers to be able to send across borders for the purpose of maintaining the security of their infrastructure.

The increased demand for data localisation means that the economies of scale where a cloud provider can use one data centre to serve many customers are degraded. The need to run and maintain more data centres can reduce the resources available for each and the ability to share knowledge, particularly around cyberthreats, between them. Maintaining the infrastructure to transfer data between countries is requiring ever more intricate procedures. Keeping up with these local regulations results in more complex technical systems and risks introducing vulnerabilities.

Data embassies might provide one means of doing this. Luxembourg signed an agreement with Estonia granting the information Estonia stores in data centres in Luxembourg the same level of inviolability and immunity as physical embassy buildings. This kind of measure is particularly important for small countries that might struggle

> "THE MAJOR PROVIDERS HAVE VERY IMPRESSIVE CAPACITY TO DEAL WITH A VARIETY OF CYBERTHREATS. THE MATURE CLOUD PROVIDERS ARE SIGNIFICANTLY AHEAD OF SMALLER, NEWER, LOCAL COMPETITORS. OFTEN, ANALYSIS OF THOSE SHOWS VULNERABILITIES.
>
> **Majid Malaika, Chief Adviser to the Vice Governor, Saudi Arabia Monetary Authority**

to establish disaster recovery data centres that are sufficiently remote to ensure they will not be affected by natural disasters.

There are increasingly popular legal means of ensuring that, at least in the event of data being requested by a foreign government, a cloud provider will inform the client. It may even be possible for central banks, particularly if operating as a collective bloc (like the Eurosystem 27) might be able to negotiate stronger legal guarantees of their data sovereignty.

However, some in the central banking community said that assurances and guarantees that data will be kept sovereign would not necessarily be sufficient to allay all of their concerns. 'For us, we would want to see operational assurances, not just legal ones,' said a central bank official who preferred to remain anonymous. 'Unless we can be confident that the cloud provider cannot expose our data even if ordered to do so, then we will not be comfortable placing it in a cloud data centre where the owner is headquartered in the US.'

This kind of technical assurance is possible. Cloud providers can offer encryption services, meaning that they store only encrypted data. Of course, if the cloud provider has access to the key, they can be ordered to decrypt it. It is possible, however, to design a system where the cloud provider does not have access to the decryption key. 'We have implemented these kinds of solutions in the past, but it requires a long and thorough architecture process and will likely result in losing desirable features provided by the cloud service/provider,' said Malaika.

However, as these demands are becoming more common, cloud providers are developing these systems to make them easier for customers to use, allowing them to technically demonstrate to regulators that they have full control over their data and the cloud provider does not. BNP Paribas relies on this type of 'keep your own key' solution for its use of public cloud infrastructure.

This kind of solution, though attractive from the perspective of ensuring data sovereignty, does come with a cost. It is much more difficult and complex to run searches and indexing on encrypted data.

Much of the analysis central banks might wish to run on their data, particularly involving AI, will be extremely difficult to conduct on encrypted data stored in the cloud. It would require the central bank either to decrypt the data within the cloud, or to replicate the cloud environment in on-premises architecture. And if the analysis needs to be conducted on premises, then the central bank may see less value in migrating to the cloud in the first place.

Looking ahead

The benefits of cloud migration are already well understood in private financial sector institutions. If properly implemented, a hybrid cloud architecture can deliver efficiency savings and improvements to security relative to on-premises architecture.

> "
>
> THE MATURE CLOUD PROVIDERS ARE SIGNIFICANTLY AHEAD OF SMALLER, NEWER, LOCAL COMPETITORS. OFTEN, ANALYSIS OF THOSE SHOWS VULNERABILITIES.
>
> **Majid Malaika, Chief Adviser to the Vice Governor, Saudi Arabia Monetary Authority**

Digital technology is becoming more sophisticated at an incredibly rapid pace. Central banks are expected to be on the cutting edge of economic forecasting, using the most sophisticated data analysis techniques. Increasingly, these require AI and machine learning, for which the computational demands are enormous. Quickly training these models is achieved most efficiently in the cloud.

Central banks must be able to avail themselves of the best technology available. Because of the procurement lifecycle, on-premises architecture is dated for much of its lifespan. Only economies of scale enable cloud providers to keep pace.

Consensus is building that, despite the additional exposure entailed by multi-tenant infrastructure, the best cloud providers can offer an improvement on security relative to on-premises architecture. Even in central banks, this conclusion is starting to be acknowledged. However, central banks and regulators remain uncertain about global cloud services providers. The availability of technical solutions to ensure sovereignty is not yet widely known or deployed in the central banking community.

The thrust of privacy regulation is to restrict either the geographic location of data centres, or to restrict the use of cloud service providers based on the location of their headquarters. These approaches risk both pushing users towards inferior local cloud providers and degrading the efficiency of global providers by impairing their ability to share data and serve customers from multiple locations with a single data centre.

Challenges remain – regulatory complexity, particularly around data privacy, is likely to continue to slow adoption. However, commercial banks, operating under many of the same restrictions, have managed to advance substantially further in their cloud migrations than central banks. It is to be hoped that, as understanding grows in the public sector around both the benefits cloud offers and the means of mitigating their outstanding concerns, the path to broader adoption can be smoothed. ■

FURTHER READING

IBM, 'Principles of a Trustworthy Cloud', May 2023

IBM, 'IBM Cloud Framework for Financial Services', September 2020

Futurum, 'Confidential Computing: The Future of Data Security and Digital Trust', October 2021

IBM, 'Cloud's next leap', October 2021

IBM, 'Mastering hybrid cloud', June 2022

IBM, 'The deep cloud alternative', August 2022

IBM, 'A comparative look at enterprise cloud strategy', September 2022

IDC, 'Gaining Insights at Scale with HPC Managed Solutions', October 2022

IBM, 'Unlocking innovation and business value for your financial institution', January 2023

IBM, 'The Next Frontier in Security: Confidential Computing'

IBM, 'Confidential computing for total privacy assurance'

American Bankers Association, 'Cloud Computing in the US Banking Industry', June 2021

Association for Financial Markets in Europe, 'Regulatory complexity is making it harder for financial institutions to adopt cloud services', December 2022

BSA, 'Korea: BSA Submission on Proposed Amendments to Cloud Security Assurance Programme', January 2023

Estonian Embassy to Luxembourg, 'Factsheet: Data Embassy'

Eurostat, 'Cloud computing – statistics on the use by enterprises', 2020-2021

International Data Corporation, 'Banking Cloud Trends in Asia/Pacific', 2022

KPMG, 'Third party and cloud: Regulatory challenges', 2022

US Treasury, 'The Financial Services Sector's Adoption of Cloud Services', February 2023

Official Monetary and Financial Institutions Forum
181 Queen Victoria St, London, EC4V 4EG. United Kingdom
T: +44 (0) 20 700 27610

enquiries@omfif.org

omfif.org/dmi

ABOUT OMFIF

With a presence in London, Washington and New York, OMFIF is an independent forum for central banking, economic policy and public investment – a neutral platform for best practice in worldwide public-private sector exchanges.

SPONSORED BY

IBM Cloud for Financial Services® is designed to build trust and enable a transparent public cloud ecosystem with the features for security, compliance and resiliency that financial institutions require. Financial institutions can confidently host their mission-critical applications in the cloud and transact quickly and efficiently. With a large partner ecosystem of independent software vendors, software as a service and fintech partners, IBM Cloud for Financial Services offers a new generation of cloud for the enterprise. Financial institutions can now deploy on public cloud to enable innovation and deliver new outstanding customer experiences, while managing stringent industry regulations for sensitive data and complex workloads.

AUTHOR

Lewis McLellan
Editor, Digital Monetary Institute

EDITORIAL AND PRODUCTION

Simon Hadley
Director, Production

William Coningsby-Brown
Production Manager

Sarah Moloney
Chief Subeditor

COMMERCIAL

Folusho Olutosin
Commercial Director, Digital Monetary Institute

ACKNOWLEDGMENTS

OMFIF thanks officials from the co-operating countries and cities for this publication, which will be joining us in launch partnerships around the world. We are grateful to many other associates and colleagues for their assistance and guidance.

Company Number: 7032533. ISSN: 2398-4236


DMI
OMFIF
Digital
Monetary
Institute