FORRESTER®

Adopt Hybrid Cloud To Resolve The False Dilemma Between Resilience And Modernization In Banking

Banking Results From The February 2024 Thought Leadership Paper, "The Path To Operational Resilience Begins With Reliability And Risk Management"

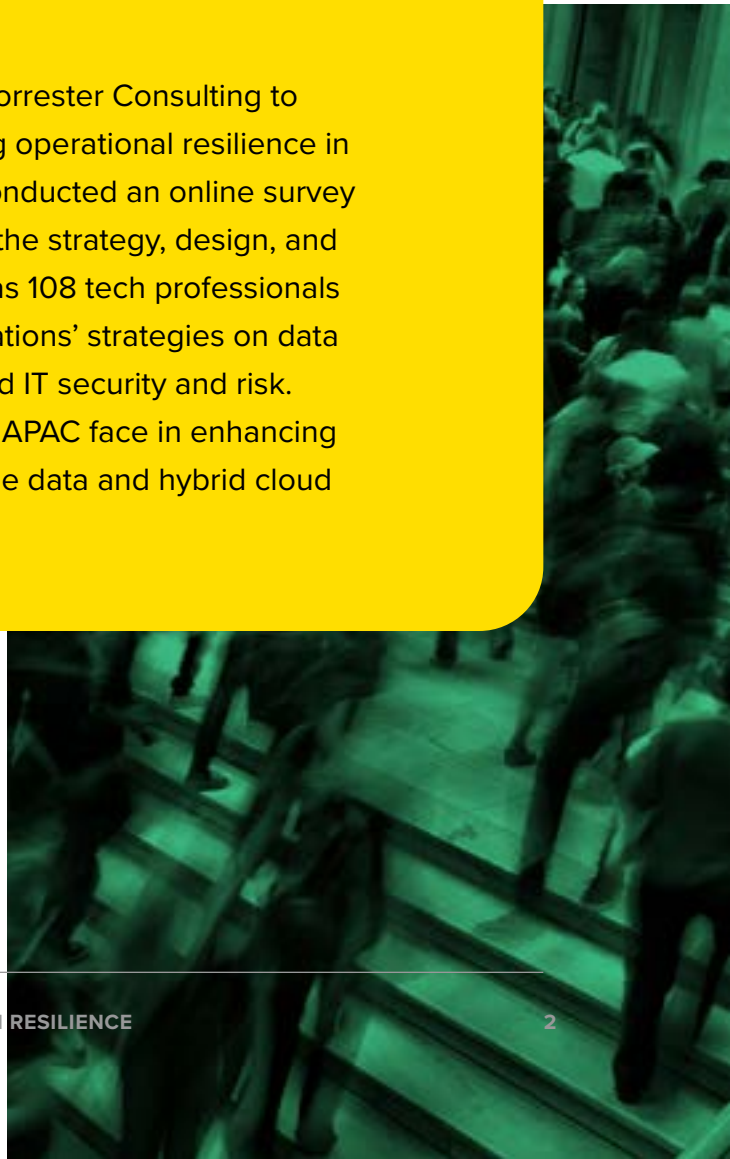
A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY RED HAT AND INTEL, MARCH 2024

Executive Summary

Frequent service disruptions, increased regulatory scrutiny and growing privacy concerns have prompted banks to ramp up efforts to address gaps in their operational resilience, particularly in their technology strategy. Many decision-makers attribute these issues to their banks' increasing reliance on third-party cloud services, especially as banks turn to the cloud to accelerate their modernization efforts. As a result, banks face two seemingly contradictory options: Do they retreat from the cloud to improve their resilience, or forge ahead with increasing their cloud presence, possibly at the cost of eroding their resilience?

Hybrid cloud can help banks deconstruct this false dilemma. By minimizing downtime, strengthening business continuity management, facilitating scalable operations, and embedding data security and compliance into cloud operations, hybrid cloud can enhance the operational resilience of banks in Asia Pacific (APAC) while they pursue their modernization goals through greater cloud adoption.

In August 2023, Red Hat and Intel commissioned Forrester Consulting to explore the role of data and hybrid cloud in building operational resilience in the financial services industry in APAC. Forrester conducted an online survey with 166 business decision-makers responsible for the strategy, design, and delivery of the organization's key services, as well as 108 tech professionals from banks who were responsible for their organizations' strategies on data infrastructure, data management, data analytics, and IT security and risk. This study will explore the challenges that banks in APAC face in enhancing operational resilience and how they plan to leverage data and hybrid cloud in building operational resilience.



Key Findings

The growing frequency of service disruptions has driven operational resilience to become a top-of-mind concern for banks. Sixty percent of business decision-makers from banks stated that their organizations had experienced at least one major service disruption over the past 12 months. This underscores the mounting pressure on banks in APAC to maintain resilient banking services.

Cloud's perceived negative impact on operational resilience has caused cloud hesitancy to set in among banks in APAC. Sixty-one percent of banking tech professionals indicated that the increasing migration of services to third-party cloud architectures has had a negative impact on their banks' operational resilience.

Hybrid cloud can help banks resolve the false dichotomy between resilience and modernization. Our study foresees a distinction emerging between decision-makers who are reluctant to engage in cloud-driven modernization at their banks due to cloud hesitancy, and those embracing hybrid cloud to advance their bank's modernization efforts and capitalize on new opportunities while maintaining operational resilience.

Operational Resilience Is A Top-Of-Mind Concern For Banks But Gaps In Technology Strategy Persist

The frequency and severity of service disruptions in APAC's banking sector has been rising in recent years. Operational resilience has thus become a central focus of bank management and boards. Even as banks introduce initiatives to upgrade internal systems and processes, resilience gaps in their technology strategy continue to pose challenges:

As service disruptions continue to grow in frequency and severity, banks are focusing on operational resilience as their top business priority. Three out of five business decision-makers (60%) reported that their organization experienced at least one major service disruption in the last 12 months. More than half of them identified that incurring financial penalties (68%) and issuing compensation to customers (56%) were the most significant consequences of these disruptions.

3 in 5 business decision-makers (60%) stated that their bank had experienced at least one major service disruption in the last 12 months.

These service disruptions — and their consequences —have prompted banks to rethink their business priorities. For banking business decision-makers, improving operational resilience is now the foremost organizational priority over the next 12 months, ahead of other objectives like improving customer experience (CX) or developing new products and services (see Figure 1).

Enhancing business continuity for critical services is a key area of concern for banks. Banking services that enable customers to conduct daily financial transactions instantaneously (e.g., e-wallet payments, credit card transactions, deposit/withdrawal services) were considered by banking business respondents to be most critical to their organization (see Figure 2).

To enhance the resilience of these services, banks are concentrating their efforts on improving their capabilities in business continuity management by developing response strategies and establishing redundancies. In fact, business continuity planning was ranked by business decision-makers as the

top element of resilience they aim to improve (31%) to enhance their ability to deliver critical financial services during a disruption.

FIGURE 1

Top 5 Organizational Priorities For Banks Over The Next 12 Months

30%
Enhance the organization's operational resilience

24%
Improve employee experience

27%
Develop new banking products to cater to changing consumer needs

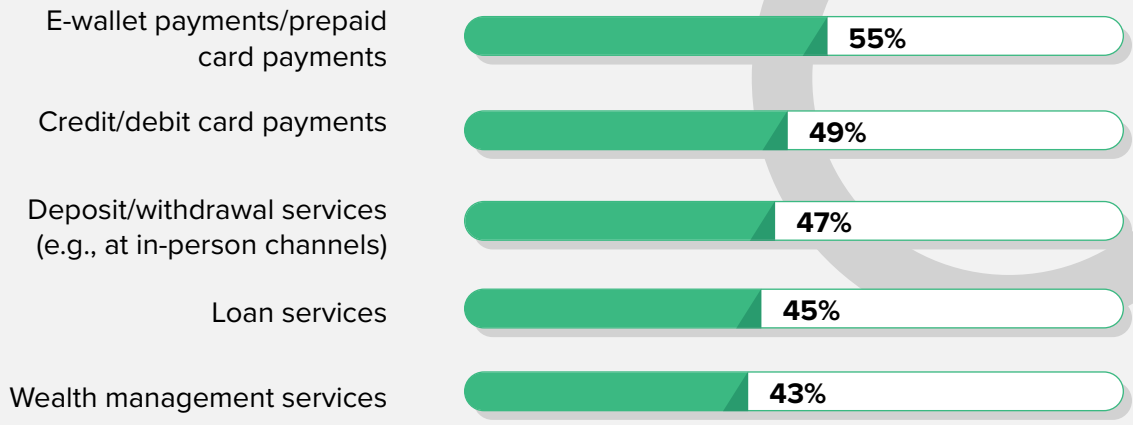
23%
Build robust and reliable banking operations

25%
Improve the overall experience of banking customers

Base: 166 business decision-makers in the APAC banking industry
Note: Showing consolidated responses for options ranked by respondents as top 3 at their banks.
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

FIGURE 2

Top 5 Most Critical Customer-Facing Services For Banks



Base: 166 business decision-makers in the APAC banking industry
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Banks face a resilience gap in their technology strategy. While banks have demonstrated their intent to improve their operational resilience, business and technology stakeholders hold divergent views on how committed banks really are to improving operational resilience. Sixty-three percent of business decision-makers believe that their bank viewed operational resilience as a key priority. In contrast, only 47% of tech professionals shared the same perspective. With business decision-makers and tech professionals occupying different vantage points within their organizations, this perception gap indicates that banks' current efforts to prioritize resilience may not sufficiently extend to their technology strategy.

Banks Anticipate That Their Use Of Public Cloud Services Will Close Tech-Related Resilience Gaps

As highlighted in our Thought Leadership Paper commissioned by Red Hat and Intel titled, "The Path To Operational Resilience Begins With Reliability And Risk Management," the rapid growth in cloud adoption was identified by decision-makers in the financial services industry as a key contributor to the erosion of operational resilience. Banks are no exception. With the emergence of digital-native financial institutions, modernization has become an imperative for banks. In response to intensifying competition, banks have enlisted third-party cloud service providers to modernize key services and improve speed-to-market. Yet, these cloud services have also introduced new challenges to operational resilience, giving rise to cloud hesitancy amongst banks:

Failures in critical third-party IT services (e.g., cloud services) are major root causes of service disruptions. As part of their modernization efforts, banks have outsourced many of their IT functions to external service providers to improve flexibility and introduce innovative new service delivery models. In fact, some banks have become almost entirely dependent on third parties for a wide range of IT services, including application development and cloud services.[1]

60%

of banking business decision-makers noted that their organization views reducing concentration risks by diversifying third-party providers of critical IT services like cloud services as a key priority.

On the other hand, third-party IT services like public cloud have introduced a variety of risks (e.g., data breaches, service disruptions) that banks cannot directly control. More than 1 in 3 banking tech professionals (35%) cited failures in critical third-party IT services as a major cause for disruptions — on-par with cybersecurity incidents. Additionally, 61% of banking tech professionals indicated that the increasing migration of services to third-party cloud architectures has had a negative impact on their banks' operational resilience.

Concentration risk in cloud services has emerged as a key concern for regulators and banks. Even among third-party IT risks, outsourced cloud services pose a unique challenge. In 2022, the Bank for International Settlements (BIS) stated that the growing reliance of financial services firms on a small number of cloud computing service providers was creating single points of failure, and hence resulting in new forms of concentration risk at the technology services level.[2] Recent outages in cloud and data center services have resulted in significant service disruptions for multiple banks in APAC, further emphasizing these concerns.

Indeed, banking business decision-makers viewed reducing concentration risks by diversifying third-party providers of critical IT services like cloud services as their top priority in improving resilience (see Figure 3).

FIGURE 3

Top 3 Actions Banks Are Prioritizing To Improve Operational Resilience

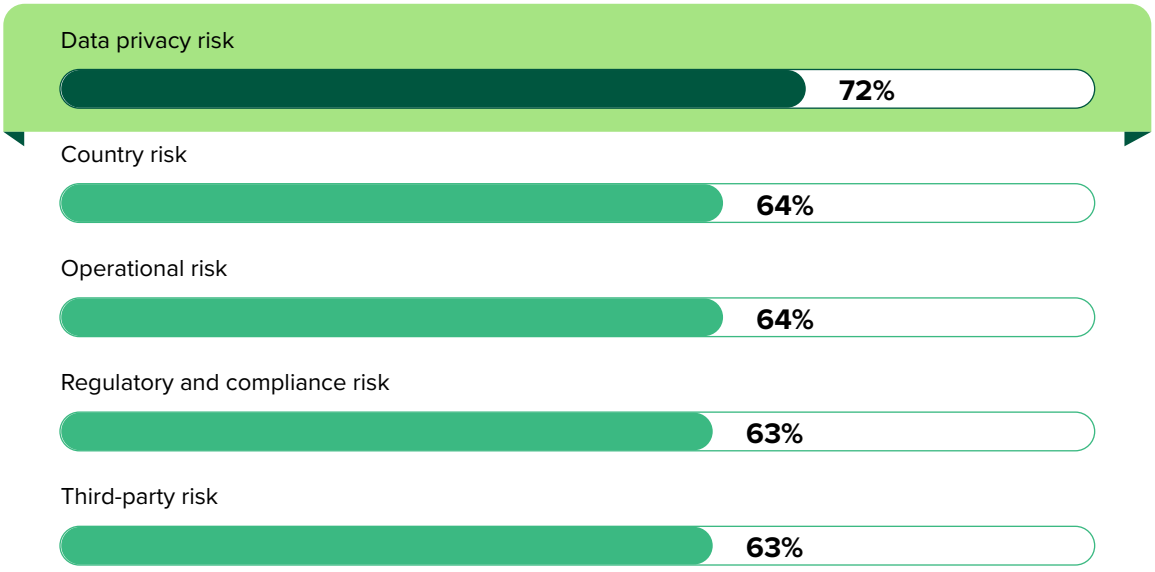
Base: 166 business decision-makers in the APAC banking industry
Note: Showing sum of responses for “Critical priority” and “High priority”
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Data sovereignty and privacy requirements introduce new complexities when using cloud services. Banking business decision-makers were most concerned about data privacy risks in their efforts to build resilience (see Figure 4). Managing data privacy risks is especially complex during cloud service disruptions as banks must ensure the confidentiality of individuals' data and prevent unauthorized access or breaches during failover operations (i.e., the process of shifting operations from one system or location to another).

In addition, many countries have data sovereignty laws that require organizations to store and process data within their national borders. This can complicate failover operations, as banks must ensure that backup or secondary systems used for failover comply with data localization requirements. Over half of banking business decision-makers (53%) reported that ensuring compliance with data residency regulations posed challenges for their banks in their efforts to enhance resilience.

FIGURE 4

Top 5 Most Challenging Risks For Banks To Manage



Base: Variable depending on the number of business decision-makers in the banking industry who had selected each risk as one of the top 5 risks they were most concerned about.
Note: Showing sum of responses for “Extremely challenging” and “Challenging”
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Cloud hesitancy has set in among banks in APAC. Turning away from cloud altogether risks enfeebling banks' modernization efforts. Furthermore, cloud computing's key role in democratizing access to new advances in data analytics and AI could risk banks losing more ground by dramatically scaling back their cloud footprint. Hence, banks are faced with a dilemma: To retreat from the cloud to improve their resilience, or to forge ahead with increasing their cloud presence, possibly at the cost of eroding their resilience.

At least for this juncture, it appears that the net effect of cloud service disruptions, regulatory scrutiny, and privacy concerns, is that banks' appetite for cloud adoption has waned, especially for core banking operations. Banking business decision-makers noted that they expect the share of core banking-related workloads deployed on public cloud (single and multiple) to decline from 52% today to 44% over the next two years. This signals a retreat from the cloud. In the context of resilience as a top-of-mind concern, this decline suggests that banks view any growth in their public cloud footprint as antithetical to their goal of fostering greater resilience. In other words, the rising focus on resilience has caused cloud hesitancy to take root among banks in APAC.

Deconstruct The False Dichotomy Of Resilience And Modernization Through Hybrid Cloud

Hybrid cloud is a powerful approach to reconcile the seemingly contradictory objectives of resilience and modernization. Hybrid cloud allows banks to combine private cloud's security and control with public cloud's scalability and cost efficiency. Banks in APAC are increasingly turning to hybrid cloud environments to resolve varied challenges arising from third-party cloud risks. Minimizing downtime, improving business continuity, enabling scalable operations, and maintaining data security and compliance, enables hybrid cloud to help APAC banks enhance their operational resilience while pursuing the goal of modernization.

Hybrid cloud offers banks a myriad of benefits related to resilience. Hybrid cloud refers to a computing environment that combines the use of both public and private cloud infrastructure. It is a strategic approach that allows organizations to leverage the benefits of both private and public clouds, while maintaining control over their data, applications, and infrastructure.

In a hybrid cloud setup, banks can choose to keep their critical data and applications on their own infrastructure (i.e., private cloud), while utilizing the public cloud for less sensitive workloads or to handle peak periods of demand. The private and public clouds are connected through secure networks, enabling seamless data exchange and application integration.

Hybrid cloud can help banks improve their resilience by:

Enhancing their business continuity and disaster recovery in the event of service outages related to public cloud. Hybrid cloud allows banks to implement robust business continuity and disaster recovery strategies for a range of scenarios, including public cloud outages. By leveraging both on-premises infrastructure and multiple public cloud services, banks can replicate critical data and applications across multiple environments. In the event of a disruption, banks can seamlessly redirect and restore operations, ensuring continuity of banking services and minimizing the impact on customers.

Allowing banks to withstand unexpected surges in demand by scaling computing resources to handle spikes in a cost-effective manner. Hybrid cloud empowers banks to scale their infrastructure and resources based on fluctuating demands. Banks can leverage the scalability and elasticity of cloud services to manage the increased load during peak periods or spikes in transaction volumes. This elasticity ensures that banking systems and applications remain responsive and available to customers, even during periods of high demand for critical banking services (e.g., e-wallet transfers, credit card transactions).

Hybrid cloud allows banks to optimize their IT costs by leveraging their cloud services' scalability and pay-as-you-go model. Banks can use cloud services for nonsensitive workloads or peak periods, reducing the need for excessive on-premises infrastructure investments.

Enabling banks to implement a cloud compliance regime that ensures data security both during everyday operations and cloud disruptions. Banks are the custodians of the customer's sensitive financial data and must abide by strict compliance requirements. Hybrid cloud allows them to segregate their data based on sensitivity and compliance needs. They can keep critical customer data and applications on-premises in a private cloud, ensuring complete control over data security; and store less sensitive data in the public cloud, enabling cost-effective scalability and flexibility. Banks will thus have greater control over their data security with hybrid cloud. They can implement their own security measures and protocols in their private cloud environment, ensuring that sensitive data is protected according to their specific compliance requirements.

> The share of core banking applications running on hybrid cloud is expected to double over the next 24 months (6% to 13%) while the share of core banking applications running on single and multiple public cloud is projected to contract over the same period (52% to 44%).

Hybrid cloud also lets banks maintain compliance with data privacy regulations during failover operations. By implementing data segregation

and control measures, businesses can ensure that sensitive data remains within the appropriate jurisdiction or region. This addresses data privacy concerns and ensures compliance with relevant regulations.

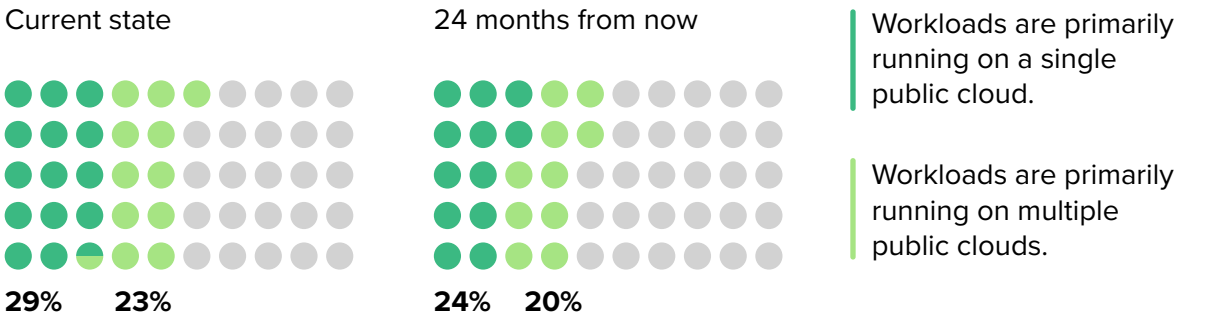
Banks are showing signs of embracing hybrid cloud to enhance operational resilience.

The percentage of core banking applications running on hybrid cloud is expected to double over the next 24 months. The percentage is expected to rise from 6% to 13%. In contrast, the average proportion of core banking applications operating on single and multiple public cloud platforms is projected to decrease during the same period, falling from 52% to 44% (see Figure 5).

This recalibration of banks' cloud strategy suggests that at least some have recognized the benefits of hybrid cloud in addressing their bank's resilience gap. As this trend gains momentum, we foresee a distinction emerging between banks that are reluctant to engage in cloud-driven modernization due to cloud hesitancy and those that are embracing hybrid cloud to advance their modernization efforts and capitalize on new opportunities while maintaining operational resilience.

FIGURE 5

Environments That Core Banking Applications Are Running On



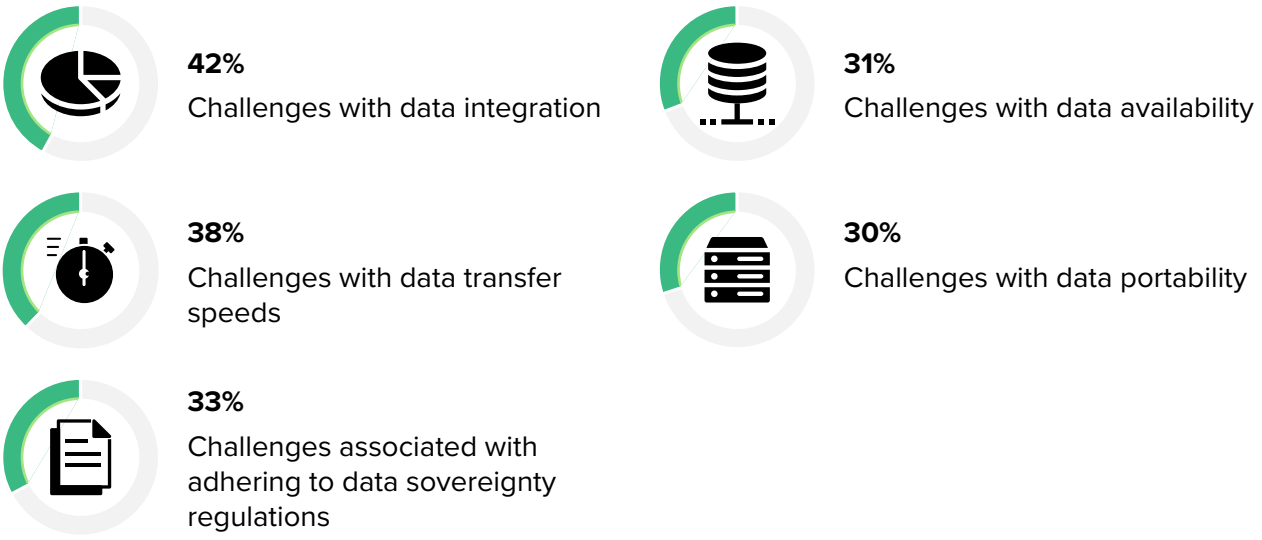
Base: 108 tech professionals in the banking industry
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Implementing hybrid cloud is not without its share of challenges. Operating in a hybrid cloud environment entails the use of multiple cloud providers, each with unique sets of APIs, data formats, and integration tools. This complexity not only makes data integration across cloud environments a formidable task but can also increase costs. Inadequate data integration can introduce new obstacles for resilience by leading to delays in monitoring and assessing risks and hindering the timely generation of alerts and notifications. Banking tech professionals agree with this view, citing data integration (42%) and data transfer speeds (38%) as top challenges their banks face in hybrid cloud environments (see Figure 6).

Addressing these challenges requires careful planning, expertise, and effective management strategies. Banks should consider partnering with experienced service providers and partners, leveraging automation and orchestration tools, and continuously evaluating and optimizing their hybrid cloud environment to overcome these challenges and maximize the benefits of hybrid cloud adoption.

FIGURE 6

Top 5 Data-Management Challenges Banks Face In Hybrid Cloud Environments



Base: 108 tech professionals in the banking industry
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Key Recommendations

The growth in frequency and severity of service disruptions have attracted regulatory scrutiny and placed the spotlight on cloud-related impediments to operational resilience. Yet, balancing the drive for modernization with the need for operational resilience has proven to be a challenging task for banking tech leaders. While it is no panacea, hybrid cloud can address many of the challenges related to resilience that emerge from cloud-related risks. Our study yielded several important recommendations:

Identify and define third-party cloud risks, especially for cloud services.

Identify potential risks associated with your third-party cloud providers, including risks related to data security, compliance, reliability, performance, and business continuity. Assess the likelihood and potential impact of each risk to prioritize your mitigation efforts. Build a strong understanding of how your cloud service providers manage business continuity and disaster recovery. Review their backup and recovery processes, redundancy measures, and their ability to quickly restore services in the event of a disruption, and evaluate if they match your bank's resiliency-related requirements.

Leverage hybrid cloud to build resilient technology infrastructure.

Hybrid cloud improves resilience by offering redundancy, geographic distribution, scalability, data protection, backup and recovery capabilities, and flexibility. It helps banks withstand disruptions, minimize downtime, and ensure continuous operations in the face of various challenges, thus enhancing their ability to deliver reliable services to users. When planning hybrid cloud implementation, conduct a thorough assessment of your bank's existing workloads and applications to determine their suitability for migration to different environments (e.g., on premises, private cloud, public cloud).

Plan for integration and interoperability.

Develop a comprehensive integration strategy to ensure seamless communication and data flow between on-premises and public cloud environments. Use APIs, middleware, and data integration tools to facilitate interoperability, communication, and data flow. Assess and validate integration points to ensure smooth operation and minimize disruptions.

Involve the right partners to support your bank's transition to hybrid cloud.

Leverage partners who can provide guidance and support throughout the hybrid cloud journey. Consider getting help from these partners to design and implement hybrid cloud architectures tailored to your bank's specific needs. Additionally, think about implementing training and certification programs to empower your bank's IT professionals with the skills and knowledge required to manage hybrid cloud environments effectively.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 166 business decision-makers and 108 tech professionals from banks in Australia, Hong Kong, India, Japan, Taiwan, and Southeast Asia (Singapore, Malaysia, Indonesia, and Thailand) to evaluate the role of data in building operational resilience. The study began in August 2023 and was completed in September 2023.

To read the full results of this study, please refer to the Thought Leadership Paper commissioned by Red Hat and Intel titled, "The Path To Operational Resilience Begins With Reliability And Risk Management."

Project Team:
Deepu Nair, Senior Market Impact Consultant

Amelia Lau, Market Impact Consultant

Contributing Research:
Forrester's Technology & Architecture research group

Appendix B: Demographics

BUSINESS DECISION-MAKERS

REGION	
Australia	**17%**
Hong Kong	**17%**
India	**16%**
Japan	**17%**
Taiwan	**7%**
Southeast Asia	**25%**

LEVEL OF RESPONSIBILITY	
Final decision-maker	**51%**
Part of a team making decisions	**31%**
Influence decisions	**18%**

NUMBER OF EMPLOYEES	
1,000 to 2,499	**0%**
2,499 to 4,999	**37%**
5,000 to 19,999	**35%**
20,000 or more	**27%**

INDUSTRY SEGMENT	
Corporate banking	**42%**
Retail banking	**37%**
Wealth management	**21%**

DEPARTMENT	
Finance/accounting	**22%**
CX	**14%**
Banking operations	**26%**
Strategy	**8%**
Business analytics	**7%**
Digital business	**7%**
Governance, risk, and compliance	**8%**
Sales	**5%**
Legal	**4%**

Appendix B: Demographics

BUSINESS DECISION-MAKERS (CONTINUED)

ANNUAL REVENUE	
$500 million to $999 million	**30%**
$1 billion to $5 billion	**43%**
More than $5 billion	**28%**

POSITION	
C-level executive	**20%**
Senior vice president/president	**41%**
Senior manager/director	**37%**

Note: Percentages may not total 100 due to rounding.

TECHNOLOGY PROFESSIONALS

REGION	
Australia	**16%**
Hong Kong	**16%**
India	**18%**
Japan	**17%**
Taiwan	**7%**
Southeast Asia	**26%**

DEPARTMENT	
IT operations	**21%**
IT infrastructure	**23%**
Application design and development	**12%**
Platform engineering	**15%**
Systems analysis	**10%**
Data engineering	**9%**
Enterprise architecture	**9%**

INDUSTRY SEGMENT	
Corporate banking	**33%**
Retail banking	**44%**
Wealth management	**18%**

POSITION	
C-level executive	**22%**
Senior vice president/president	**48%**
Senior manager/director	**30%**

NUMBER OF EMPLOYEES	
1,000 to 2,499	**0%**
2,499 to 4,999	**39%**
5,000 to 19,999	**37%**
20,000 or more	**24%**

ANNUAL REVENUE	
$500 million to $999 million	**22%**
$1 billion to $5 billion	**41%**
More than $5 billion	**37%**

TECHNOLOGY PROFESSIONALS (CONTINUED)

LEVEL OF RESPONSIBILITY (DATA INFRASTRUCTURE)	
Final decision-maker	**70%**
Part of a team making decisions	**19%**
Influence decisions	**7%**

LEVEL OF RESPONSIBILITY (DATA ANALYTICS)	
Final decision-maker	**36%**
Part of a team making decisions	**44%**
Influence decisions	**12%**

LEVEL OF RESPONSIBILITY (DATA MANAGEMENT)	
Final decision-maker	**35%**
Part of a team making decisions	**45%**
Influence decisions	**16%**

LEVEL OF RESPONSIBILITY (IT SECURITY AND RISK)	
Final decision-maker	**43%**
Part of a team making decisions	**29%**
Influence decisions	**12%**

Note: Percentages may not total 100 due to rounding.

Appendix C: Endnotes

[1] Source: "The State Of Cloud In Financial Services, 2023," Forrester Research, Inc., April 25, 2023.

[2] Source: Bank For International Settlements, Big tech interdependencies — a key policy blind spot, July 5, 2022.