FORRESTER®

The Path To Operational Resilience Begins With Reliability And Risk Management

Hybrid Cloud And Data Availability Are Crucial To Building Operational Resilience For Financial Services Firms In Asia Pacific (APAC)

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

Table Of Contents

Project Team:

Deepu Nair, Senior Consultant

Alicia Choo, Market Impact Consultant

Amelia Lau, Market Impact Consultant

Contributing Research:

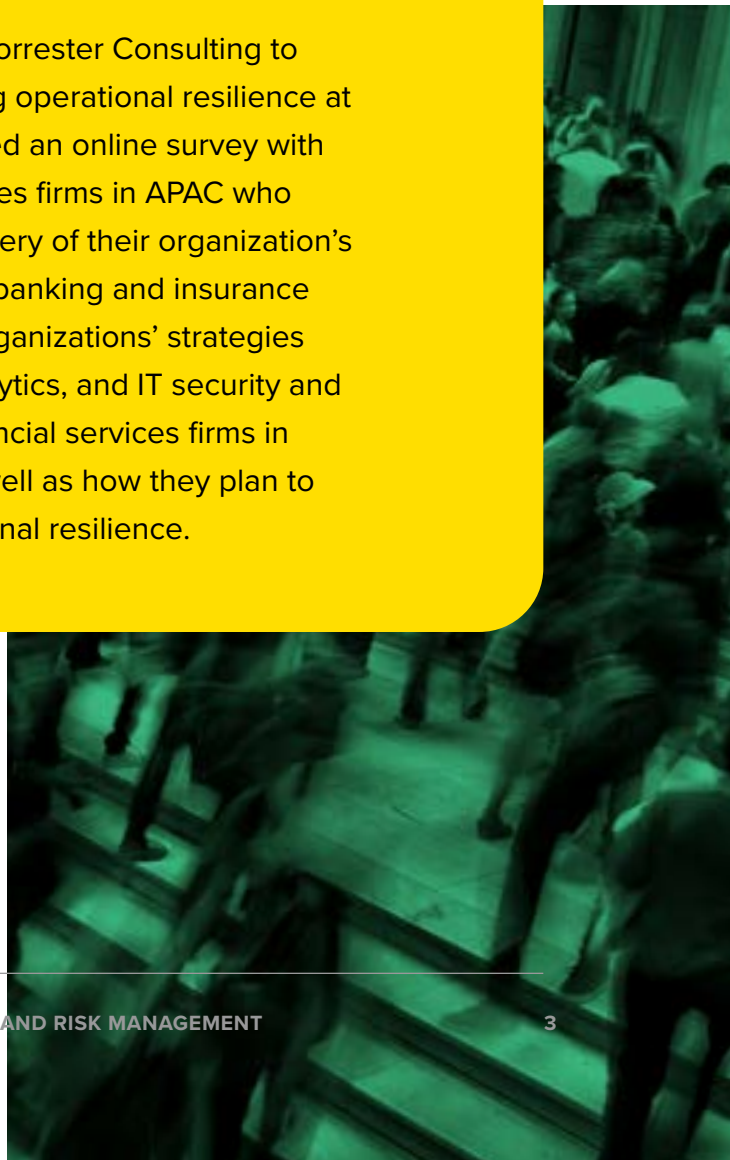
Forrester's Technology & Architecture research group

Executive Summary

In the past year, major service disruptions in APAC have spotlighted the need to improve operational resilience within the financial services industry. Two key drivers emerge as the root causes of the financial services industry's recent decline in operational resilience, namely: The complexities associated with the growth in cloud adoption, and the rapid expansion in the number and complexity of applications and data sources.

Current approaches to improve resilience at financial services firms are highly reactive — they prioritize recovery over proactively managing risks and enhancing reliability. To build effective operational resilience, financial services firms should adopt a two-pronged solution. First, they should implement hybrid cloud adoption to improve their technology infrastructure's reliability by mitigating cloud-related risks. Then, they must enhance data availability to stitch information from across the organization together to continuously identify, anticipate, and manage complex risks.

In August 2023, Red Hat and Intel commissioned Forrester Consulting to explore the role of data and hybrid cloud in building operational resilience at financial services firms in APAC. Forrester conducted an online survey with 330 business decision-makers from financial services firms in APAC who were responsible for the strategy, design, and delivery of their organization's key services, and with 214 tech professionals from banking and insurance verticals in APAC 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 financial services firms in APAC face in enhancing operational resilience as well as how they plan to leverage data and hybrid cloud in building operational resilience.



Key Findings

There is an urgent need for financial services firms in APAC to address gaps in operational resilience. A sharp rise in disruptions to critical services over the past 12 months has introduced growing pressure on FSI firms in APAC to adopt a more proactive approach in enhancing operational resilience.

Digital transformation and modernization have introduced new challenges to operational reliability. As new digital services usher in additional complexity, FSI firms in APAC face the daunting task of finding the right balance between meeting the demands of digital transformation and maintaining operational resilience.

Limited data availability hinders proactive risk management. Identifying, managing, and resolving risks lie at the heart of resilience. However, most FSI firms struggle to collate and analyze data related to risks associated with operational resilience. As a result, visibility over risk-related data is often incomplete, fragmented, or obsolete.

Build operational resilience by embracing hybrid cloud and enhancing data availability. Improving operational resilience requires a two-pronged approach of adopting hybrid cloud and enhancing data availability. This will improve the reliability of the tech infrastructure as well as proactively understand and manage risks associated with operational resilience.

Service Disruptions In APAC's Financial Services Industry Highlight A Need To Address Gaps In Operational Resilience

Financial services firms in APAC have encountered significant challenges in maintaining resilient services in recent times. As financial services firms across the region experienced serious service outages in recent months, it has become critical to prioritize operational resilience. However, financial services firms have traditionally adopted a compliance-driven mindset in their approach to operational resilience, primarily focused on avoiding regulatory penalties. This approach often overlooks the broader impact of resilience on customer trust. In our study, we found that:

More than 3 in 5 business decision-makers (63%) stated that their bank had experienced at least one major service disruption in the last 12 months.

Service disruptions are becoming increasingly commonplace. Sixty-three percent of financial services business decision-makers indicated that their organization has experienced a major disruption in critical services over the past 12 months. Leading causes of these disruptions as identified by financial services technology professionals include failures in critical IT services (40%), network failures (39%), cybersecurity breaches (38%), and process and control failures (37%) (see Figure 1).

It is a key challenge for financial services firms to consistently meet operational SLAs. Only a third of financial services business decision-makers (33%) believe that their organizations can consistently meet or exceed operational SLAs for customer-facing services. An even lower proportion (18%) of technology professionals believe the same, highlighting the urgency for organizations to prioritize building operational resilience (see Figure 2).

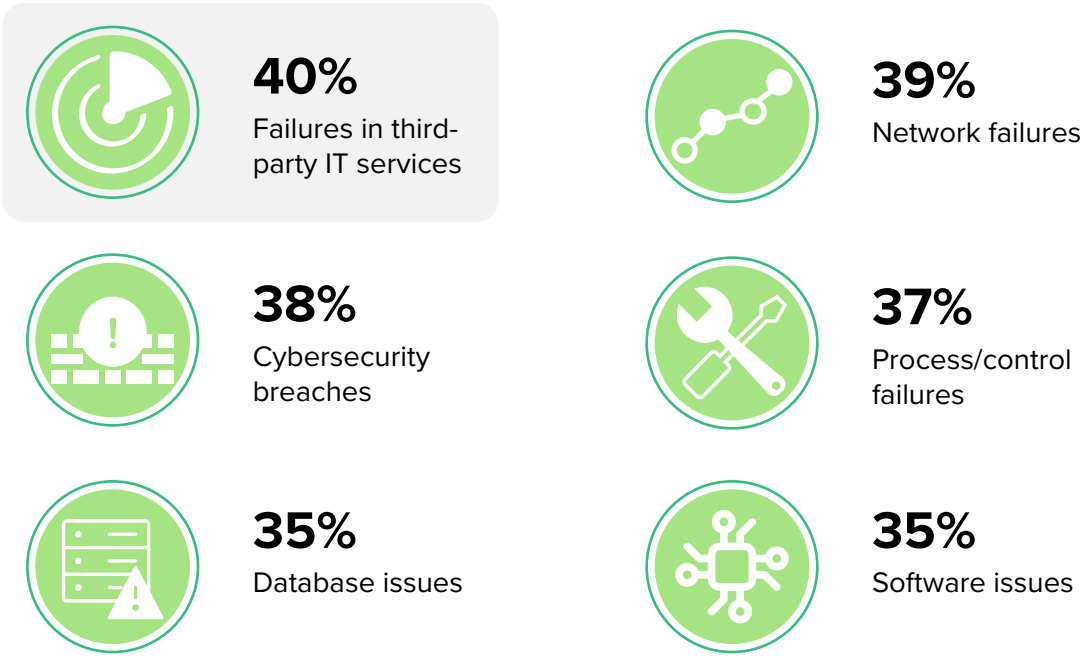
Financial services firms exhibit a compliance-driven mindset with respect to resilience. Recent service disruptions have also prompted increased regulatory scrutiny. The European Commission has introduced the Digital Operational Resilience Act (DORA) in the EU, and agencies such as the Hong Kong Monetary Authority, Australian Prudential Regulation Authority,

the Reserve Bank of India, and the Monetary Authority of Singapore have followed suit with similar guidelines. Therefore, it comes as no surprise that financial services firms operating in these highly regulated spaces are primarily focused on regulatory consequences. Seventy-three percent of financial services business decision-makers consider financial penalties to be the most critical consequence of any service disruption, followed by the compensation of customers' financial losses.

Even as financial services firms strive to improve operational resilience, their myopic focus on regulatory requirements may constrain their ability to fully appreciate the wider ramifications of service disruptions. For instance, financial services business decision-makers appear to overlook the impact of service disruptions on customer trust, with only 33% of respondents citing it as a critical consequence — suggesting the belief that service disruptions have a limited and short-term impact on customer trust.

FIGURE 1

Top 6 Root Causes Of Service Disruptions Over The Last 12 Months



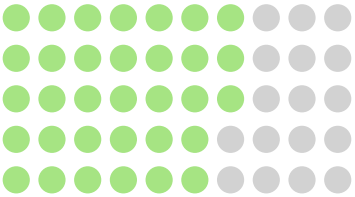
Base: 171 tech professionals from financial services firms in APAC whose organization had experienced a major service disruption for critical functions over the last 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

FIGURE 2

Financial Services Firms' Ability To Consistently Meet Or Exceed Operational SLAs For Critical Services

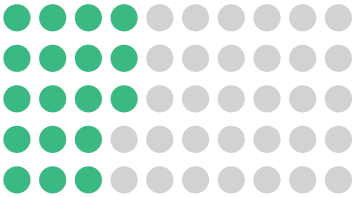
Business decision-makers

33%



IT professionals

18%



Base: 330 business decision-makers and 211 tech professionals from financial services firms in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Digital Transformation And Modernization Efforts Introduce New Challenges In Maintaining Operational Reliability

As competition in the financial services industry intensifies, digitalization has become imperative for financial services firms in APAC. As they strive to implement innovative new services and modernize existing offerings to contend with new entrants like digital banks and other fintech and insurance technology (insurtech) firms, they face a difficult task in finding the right balance between revamping their technology architecture and maintaining operational reliability:

65%

of technology decision-makers stated that the increasing migration of services to third-party cloud architectures has had a negative impact on their firms' operational resilience.

Financial services firms have significantly accelerated their adoption of cloud computing in recent years.
The initial wave of cloud adoption in the financial services industry was mostly limited to digital-native companies. There was a consensus that such endeavors were too risky, complex, and costly. However, these concerns have now been overshadowed by a renewed interest in transformation and the utilization of digital technologies in various ways to enhance efficiency, innovate propositions, and increase customer value. Today, Forrester's research indicates that financial services firms are among the heaviest of software as a service (SaaS) and public cloud platform users — more than twice the percentage of financial services firms in APAC (28%) spend between US$75 million to US$250 million on their organization's use of public cloud every year, compared to firms from other verticals in APAC (12%).[1]

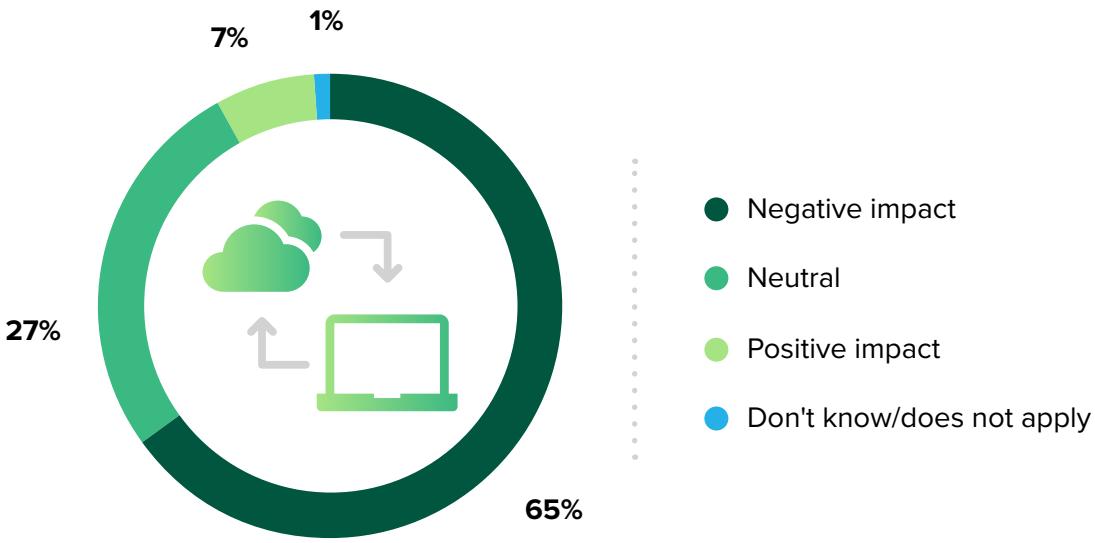
The growth in cloud adoption has given rise to new risks for financial services firms. While cloud adoption confers numerous benefits such as lower initial cost curves and reduced time to market for new services, it has ushered in fresh complications for financial services firms as well. For instance, they may face service disruptions if their cloud service providers experience outages that lead to a loss of access to their data

and applications. Migrating data to the cloud can also cause issues with meeting regulatory obligations (e.g., data residency, data sovereignty, and compliance with privacy and security regulations). Additionally, cloud adoption may result in a weakened ability to monitor data usage, access controls, and data sharing practices, all of which increases the chances of security breaches and the creation of shadow data.

Sixty-five percent of tech professionals agreed with this view, indicating that the increasing migration of services to third-party cloud architectures has had a negative impact on their firms' operational resilience (see Figure 3).

FIGURE 3

Cloud Migration's Impact On Operational Resilience



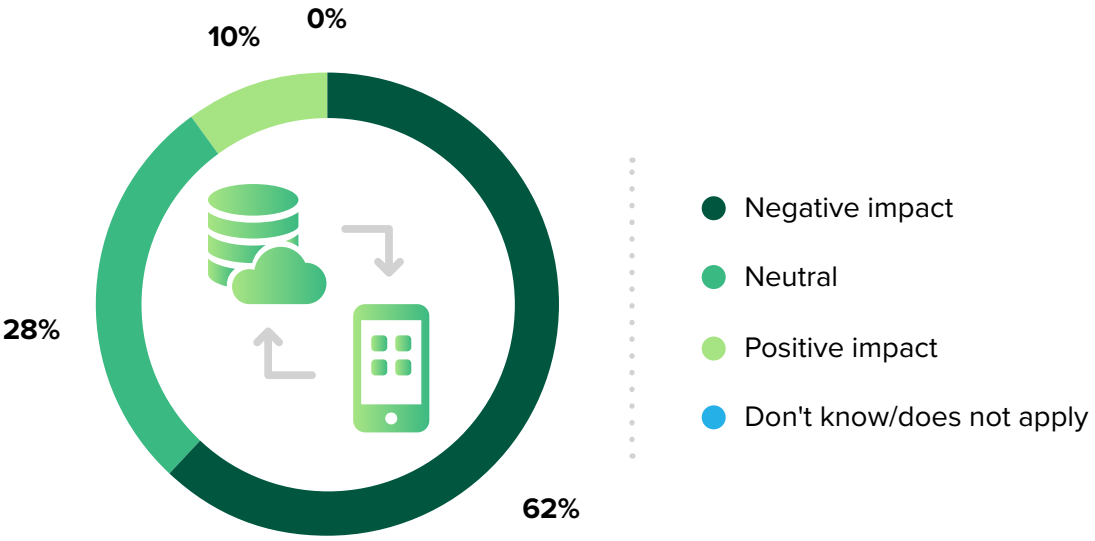
Base: 214 tech professionals from financial services firms in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

The proliferation of applications and data sources presents fresh obstacles for operational resilience. The rapid acceleration of digital transformation has significantly increased both the volume and complexity of these applications and data sources. As the number of applications and data sources increases, so does the interdependence between them. Changes

or failures in one application or data source can have a cascading effect on others, leading to widespread disruptions. Integrating disparate applications and managing complex data flows can introduce further risks such as data inconsistencies, data quality issues, or data integration failures. Sixty-two percent of technology professionals indicated that their organization's level of resilience had been adversely impacted by the rapid expansion in applications and data sources (see Figure 4).

FIGURE 4

Impact Of The Growth Of Apps And Data Sources On Operational Resilience



Base: 214 tech professionals from financial services firms in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Limited Data Availability Hinders Proactive Risk Management

Identifying, managing, and resolving risks lie at the heart of operational resilience. This allows organizations to proactively control risks instead of reacting to their downstream consequences. However, most financial services firms struggle to collate and analyze data on risks associated with operational resilience. As a result, visibility over such data is often incomplete, fragmented, and obsolete. These data voids make it difficult for financial services firms to consolidate a holistic view on risks, which is a key prerequisite for proactive risk control.

Financial services firms tend to adopt a largely reactive stance toward operational resilience. The Principles for Operational Resilience (POR) issued for financial services firms by the Basel Committee on Banking Supervision recommend that financial services firms should focus both on proactive (i.e., identifying and monitoring sources of risk) and reactive (i.e., incident response and disaster recovery) measures to building operational resilience.[2]

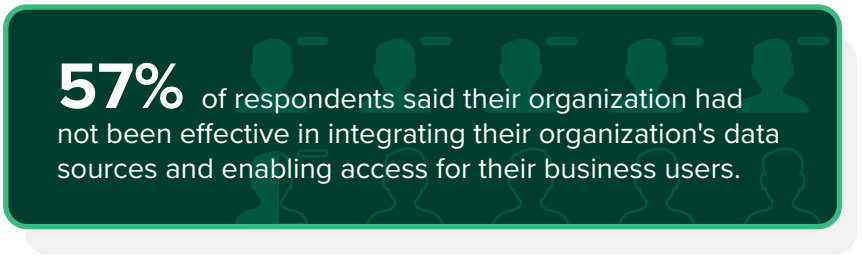
However, financial services firms often adopt a reactive approach to operational resilience, partly due to the financial consequences of recovery delays. For instance, business decision-makers identified business continuity planning as the most pressing element for improvement in building operational resilience (32%), compared to factors like implementing a resilient governance structure (15%) or an ongoing monitoring of critical IT assets (15%). Nevertheless, financial services firms' adoption of a more reactive approach is also driven in part by their inability to effectively stitch data together across the organization, making it harder for them to proactively understand and address underlying causes of operational instability.

Issues with data availability impede financial services firms' ability to collate and analyze essential risk-related data from various sources. Poor data availability can impede the organization's ability to monitor and analyze essential risk-related data from various departments in a timely manner.

In addition, poor data availability can also introduce delays in the analysis of root causes and/or the full scope of service disruptions. A majority of business decision-makers (57%) indicated that their organizations were not highly effective at integrating various data sources across the organization and enabling business users to access all relevant data sources (see Figure 5). Financial services firms' reactive approach to resilience can be linked to their inability to effectively stitch data across their organization.

FIGURE 5

"To the best of your knowledge, how effective has your organization been in integrating various data sources across the organization and enabling business users to access all relevant data sources?"



Base: 330 business decision-makers from financial services firms in APAC
Note: Only showing responses for "Not highly effective".
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Breaking down data silos and eliminating data hoarding remains a challenge. Fifty-three percent of financial services business decision-makers note that breaking down data silos and eliminating data hoarding is a key challenge for their organization, suggesting that they struggle with making risk-related data readily available across the organization (see Figure 6). Poor data availability can impede the fostering of a data-driven decision-making culture, which was also flagged as a major challenge by most business decision-makers (53%).

Collating data beyond the organization and across the ecosystem is fast becoming critical to operational resilience. With a growing number of financial services firms introducing service offerings in partnership with a wider ecosystem of partners, the availability of external data from third parties will be critical in enabling end-to-end visibility of operations across

ecosystem partners (e.g., service providers, channel partners).

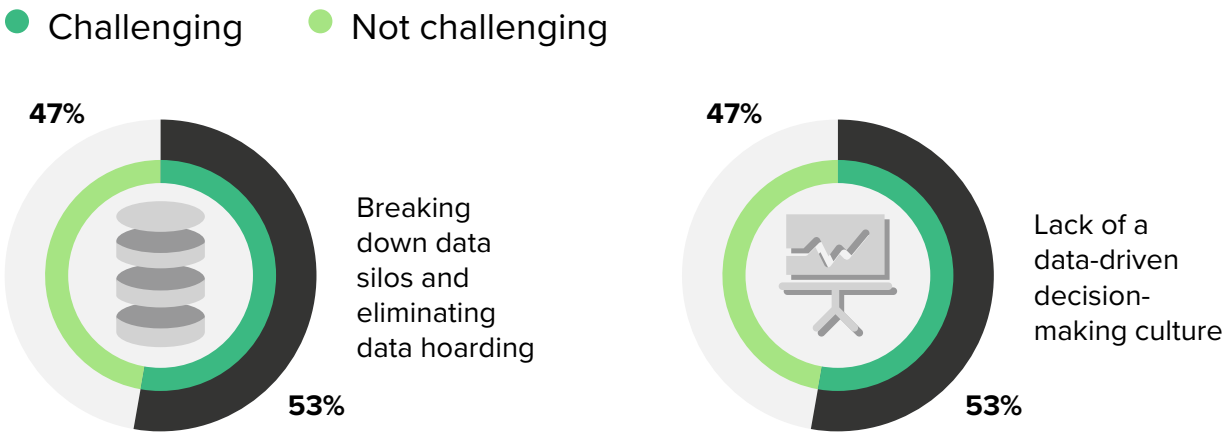
For example, banks collaborate with industry utilities that provide critical infrastructure and services. These utilities can include payment gateways and clearinghouses. Banks rely on the external data provided by these utilities for seamless and resilient operations. Analyzing payment transaction data from payment gateway partners helps banks identify patterns in the demand for cashless payments in the broader marketplace and plan for demand spikes accordingly.

Collating data from external sources also plays an important role in managing operational risks associated with processes (e.g., fraud management and anti-money laundering). Delays in receiving adverse media screening data from partners may introduce disruptions to know-your-customer (KYC) processes, leading to knock-on effects on account opening and loan issuance processes.

Survey respondents agree with the importance of obtaining data from partners — 6 in 10 business decision-makers indicated that having access to external data from third parties is essential in building operational resilience.

FIGURE 6

"How challenging have the following data-related issues been in your organization's efforts to improve operational resilience?"



Base: 214 tech professionals from financial services firms in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Build Operational Resilience By Embracing Hybrid Cloud And Enhancing Data Availability

As covered in the preceding sections, the rapid adoption of cloud computing and the proliferation of applications has impeded financial services firms' efforts to build reliable infrastructure. Simultaneously, the complexity associated with aggregating risk-related data has compounded the difficulty of comprehending and planning for crucial operational risks.

As such, financial services firms must improve the reliability of their overall technology infrastructure in the event of operational disruptions by adopting hybrid cloud to improve redundancy and dependability. However, hybrid cloud adoption on its own is not a panacea for achieving true operational resilience.

To address gaps in proactive risk management, financial services firms must also enhance data availability across their organization. Broader access to data enables the discovery, analysis, and mitigation of previously unidentified or underestimated risks. Pursuing this two-pronged approach allows financial services firms to strike a more effective balance between reactive and proactive risk management strategies.

HYBRID CLOUD IMPROVES RELIABILITY IN FSI FIRMS BY ENHANCING REDUNDANCY AND RECOVERY CAPABILITIES.

Hybrid cloud approaches help financial services firms mitigate concentration risk by allowing them to shift workloads and data to another provider in the event of an outage or disruption in the primary cloud environment. Additionally, hybrid cloud lets organizations harness multiple cloud regions or data centers located in different geographic locations. These redundancies ensure that data is replicated and accessible from various locations, thereby reducing the risk of data loss or unavailability due to regional disruptions or outages. Furthermore, hybrid cloud equips organizations with the capability to implement stringent security measures and compliance controls that align with data localization and privacy regulations. This ensures that critical data can be accessed and utilized even during disruptions, when compliance is of utmost importance.

financial services firms are increasingly embracing hybrid cloud approaches to distribute workloads across on-premise, private cloud, and public cloud environments to manage the aforementioned risks. For instance, banking tech professionals anticipate that the share of core banking workloads running on hybrid cloud environments will more than double, increasing from 6% to 13% over the next 24 months.

ENHANCEMENTS IN DATA AVAILABILITY ARE CRUCIAL IN ASSISTING FINANCIAL SERVICES FIRMS IN USING EFFECTIVE RISK MONITORING AND CONTROL TO PROACTIVELY ADDRESS OPERATIONAL RISKS.

The timely availability of data enables organizations to monitor and analyze indicators of emerging risks. This allows organizations to identify early warning signs and take proactive measures to address emerging risks before they escalate into significant threats. Moreover, increased data availability supports more advanced risk modeling and analytics. Organizations can utilize sophisticated analytical tools and techniques to analyze vast datasets and identify patterns, correlations, and outliers. A deeper understanding of risks will aid in developing more accurate risk models for predicting and managing potential threats.

Additionally, improvements in data availability can empower financial services firms to track cloud usage, costs, and performance metrics on an ongoing basis. Real-time monitoring and reporting lets financial operation teams in financial services firms identify cost-saving opportunities, detect anomalies, and take proactive measures to ensure that efforts to enhance resilience through hybrid cloud usage are conducted in a financially-optimized fashion.

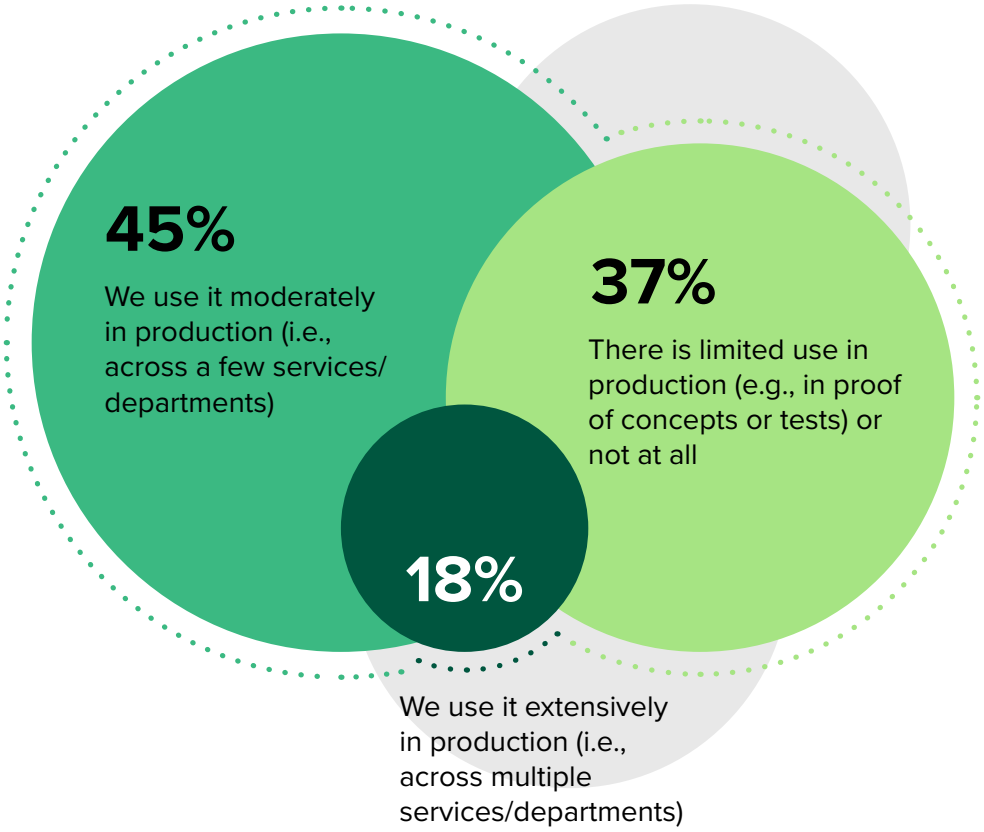
While hybrid cloud can also enhance data availability, financial services firms can also further improve data availability by investing in data management tools, establishing robust data governance frameworks, and adopting data integration platforms.

One innovative approach that financial services firms are beginning to explore is a decentralized data approach. This approach helps eliminate data silos and facilitates real-time data availability through distributed

data storage and processing, along with decentralized data ownership. Approximately 45% of respondents have indicated that their organization has started to implement data decentralization approaches in a limited manner across a few services or departments (see Figure 7).

FIGURE 7

Financial Services Firms' Adoption Levels Of Data Decentralization For Core Applications



Base: 214 tech professionals from FSI firms in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat and Intel, September 2023

Key Recommendations

Growing cloud adoption and the rapid expansion in the number and complexity of applications and data sources by financial services firms have increased service disruptions and attracted regulatory scrutiny. As a result, financial services firms in APAC are striving to enhance their operational resilience. However, many adopt a narrow view of resilience, focusing primarily on business continuity or disaster recovery. True operational resilience requires a two-pronged approach of adopting hybrid cloud and enhancing data availability to improve their tech infrastructure's reliability and proactively understand and manage operational risks. Our study yields several important recommendations:

Adopt a proactive mindset with respect to resilience.

Beyond business continuity and disaster recovery, true resilience involves improving the organization's adaptability to emerging threats by managing risks, mapping dependencies, and improving the reliability of processes and systems. Boards and senior management in financial services firms must play a key role in effecting a mindset shift away from resilience as a compliance-driven activity to one that reimagines resilience as a core organizational capability underpinned by a culture of data sharing and data-driven decision making.

Leverage hybrid cloud to build reliable technology infrastructure.

Hybrid cloud can empower financial services firms to enhance their operational resilience by increasing availability, enabling disaster recovery, providing scalability and elasticity, offering flexibility and agility, and improving data protection. Most critically, hybrid cloud can help financial services firms manage concentration risk and mitigate the impact of any potential vendor-specific disruptions. When implementing hybrid cloud, financial services firms should develop a well-defined migration strategy, including data validation and

testing, to ensure a smooth transition without data loss or disruption.

Improve data availability to enhance proactive risk management.

Leveraging comprehensive and accurate data enables organizations to make data-driven decisions, detect risks in real time, implement early warning systems, conduct advanced analytics, and enhance overall risk-management practices. This proactive approach helps organizations proactively identify, assess, and manage risks before they escalate, thereby improving operational resilience.

Augment technology initiatives with change management processes and data governance structures.

When improving data availability, financial services firms should establish clear data governance policies and standards to ensure consistency, quality, and security across data sources. financial services firms should also provide training and support to users and teams involved in using data for risk analysis. This will ensure proper understanding and utilization of data sources, and build a culture of data sharing and discovery. When working with vendors or partners for external data sources, establish clear communication channels, agreements, and data access protocols.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 330 business decision-makers and 214 tech professionals from FSI organizations in Australia, Hong Kong, India, Japan, Taiwan, and Southeast Asia (i.e., 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.

Appendix B: Demographics

BUSINESS DECISION-MAKERS

REGION	
Australia	**16%**
Hong Kong	**17%**
India	**17%**
Japan	**16%**
Taiwan	**6%**
Southeast Asia	**24%**

DEPARTMENT	
Finance/accounting	**16%**
Customer experience	**15%**
Banking operations	**13%**
Insurance operations	**12%**
Strategy	**10%**
Business analytics	**9%**
Digital business	**9%**
Governance, risk, and compliance	**8%**
Sales	**5%**
Legal	**3%**

Note: Percentages may not total 100 due to rounding.

INDUSTRY SEGMENT	
Banking	**50%**
Insurance	**50%**

LEVEL OF RESPONSIBILITY	
Final decision-maker	**48%**
Part of a team making decisions	**31%**
Influence decisions	**21%**

NUMBER OF EMPLOYEES	
1,000 to 2,499	**14%**
2,499 to 4,999	**30%**
5,000 to 19,999	**33%**
20,000 or more	**22%**

ANNUAL REVENUE	
$500 million to $999 million	**29%**
$1 billion to $5 billion	**45%**
More than $5 billion	**26%**

POSITION	
C-level executive	**18%**
Senior vice president/president	**48%**
Senior manager/director	**35%**

Appendix B: Demographics

TECHNOLOGY PROFESSIONALS

REGION	
Australia	**16%**
Hong Kong	**17%**
India	**16%**
Japan	**16%**
Taiwan	**8%**
Southeast Asia	**27%**

DEPARTMENT	
IT operations	**24%**
IT infrastructure	**23%**
Application design and development	**13%**
Platform engineering	**13%**
Systems analysis	**9%**
Data engineering	**9%**
Enterprise architecture	**8%**

LEVEL OF RESPONSIBILITY (DATA INFRASTRUCTURE)	
Final decision-maker	**64%**
Part of a team making decisions	**20%**
Influence decisions	**8%**

LEVEL OF RESPONSIBILITY (DATA MANAGEMENT)	
Final decision-maker	**32%**
Part of a team making decisions	**44%**
Influence decisions	**17%**

Note: Percentages may not total 100 due to rounding.

INDUSTRY SEGMENT	
Banking	**50%**
Insurance	**50%**

POSITION	
C-level executive	**18%**
Senior vice president/president	**50%**
Senior manager/director	**32%**

NUMBER OF EMPLOYEES	
1,000 to 2,499	**14%**
2,499 to 4,999	**34%**
5,000 to 19,999	**31%**
20,000 or more	**21%**

ANNUAL REVENUE	
$500 million to $999 million	**29%**
$1 billion to $5 billion	**41%**
More than $5 billion	**31%**

LEVEL OF RESPONSIBILITY (DATA ANALYTICS)	
Final decision-maker	**40%**
Part of a team making decisions	**37%**
Influence decisions	**14%**

LEVEL OF RESPONSIBILITY (IT SECURITY AND RISK)	
Final decision-maker	**47%**
Part of a team making decisions	**24%**
Influence decisions	**12%**

Appendix C: Endnotes

[1] Source: "Best Practices For Financial Services In Cloud," Forrester Research, Inc., February 21, 2023.

[2] Source: Bank For International Settlements, "Principles for operation resilience — Executive Summary," September 29, 2022.


FORRESTER®