Fast-Moving Clouds

10 ways to meet the promise of **hybrid** and **multicloud** in an accelerated cloud journey for financial services digital transformation

AN IDC INFOBRIEF
AUGUST 2021

IDC Financial Insights

Sponsored by Red Hat | intel

IDC Doc. #AP241258IB

Five key drivers of faster cloud adoption in 2021 and beyond

Cloud-first ambitions

More financial services institutions (FSIs) have made cloud-first strategies more real by creating connected cloud architectures, ensuring cloud-native applications and multicloud resources are integrated. According to IDC Financial Insights research, at least 40% of FSIs in Southeast Asia are already classifying themselves as cloud-first.

Need for speed

Extreme competition for product-to-market means cloud is becoming more appealing for the promise of decreased provisioning time.

Regulatory support

Beyond pre-2020 themes of regulatory clarity, new guidelines from regulators in the Asia/Pacific region are significantly more supportive of cloud, provided there is evidence of greater control and governance by the financial institution.

More business benefits

FSIs have moved beyond cost as the primary consideration as their cloud experience grows:

- App performance (response time and latency)
- Staff reskilling opportunities
- Automation for efficiency and speed of delivery
- Comprehensive security
- Risk management
- Cloud resiliency

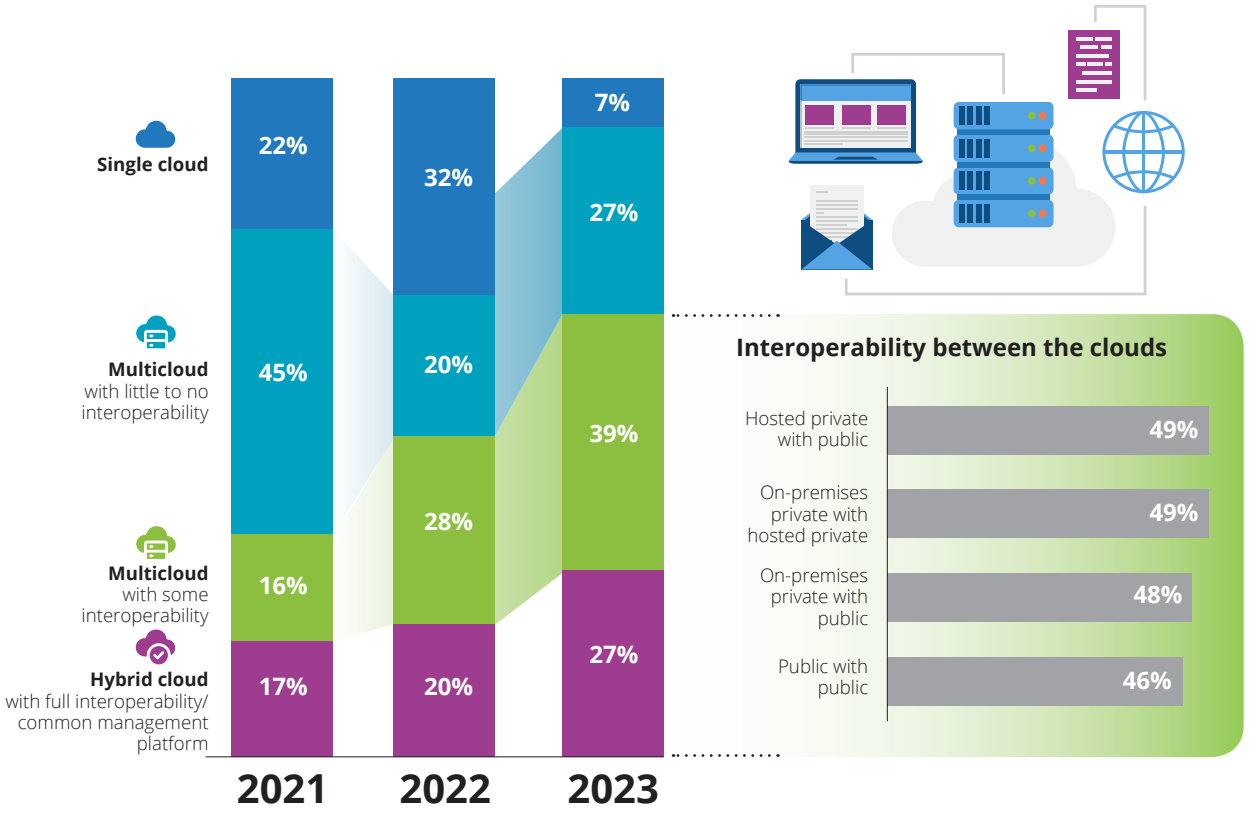
Supply-side readiness

Hyperscalers' readiness and breadth of experience are driving the acceleration of cloud deployments as customers benefit from more cost-effective resources, reliability, and scalability.

Hybrid and multicloud dominate FSIs' choice of use

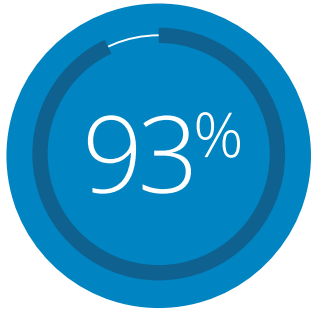
An inflection point for hybrid and multicloud environments is expected in the next two years.

How would you describe your organization's use of different on- and off-premises cloud environments?



Source: IDC Cloud Pulse Surveys (n=115, 2019), (n=104, 2020) and (184, 2021 FSIs, APeJ)

Already hybrid, and even more so in the future



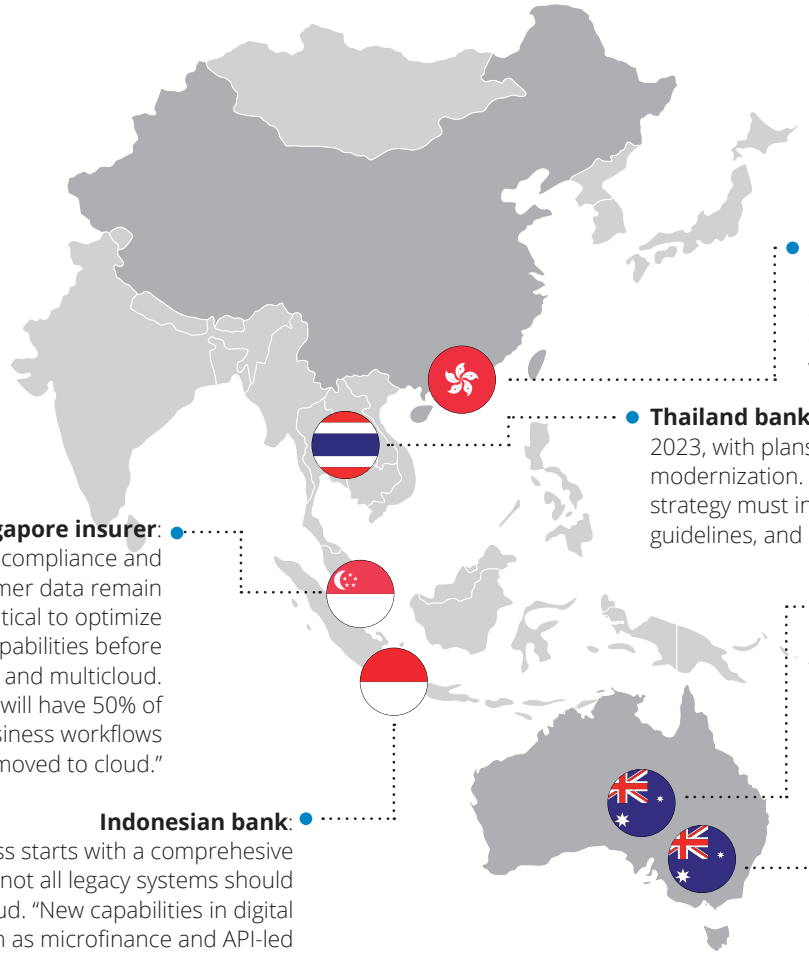
of Asia/Pacific FSIs expect to operate on hybrid and multicloud environments in 2023

Hybrid cloud is a heterogenous cloud environment where a single application runs seamlessly across the different clouds using a common set of tools and processes to support application operations.

Multicloud is a mix of multiple private and/or public cloud environments where the workloads and data have limited interoperability between the clouds.

Experiences of industry cloud leaders offer lessons on what works

To better understand the cloud practitioner's point of view, IDC handpicked six FSIs that are further in their cloud journey to be part of the first-ever IDC Financial Insights Cloud Council. The following pages present their collective experiences.



Hong Kong insurer: Has a goal for 90% of all capable workloads to be on cloud by 2022. "Legacy core applications will stay on-premises for now; all other cloud-capable workloads will move to cloud."

Thailand bank: Moving 100% to cloud by 2023, with plans to include core banking modernization. "A cloud-first banking strategy must include frameworks, guidelines, and cost benefits."

Singapore insurer: Regulatory compliance and protection of customer data remain top priorities. It is critical to optimize private cloud capabilities before expanding to public and multicloud. "By end-2022, we will have 50% of our non-core business workflows moved to cloud."

Indonesian bank: Cloud readiness starts with a comprehesive assessment; not all legacy systems should move to cloud. "New capabilities in digital banking such as microfinance and API-led banking are going on cloud first."

Australia bank: Started the cloud journey in 2013; focused on reducing complexity and pursuing the benefits of technology standardization. "Cloud is not a magic wand. It's all about automation with cloud-native applications."

Australia bank: Cloud alone is not a differentiator — how you are leveraging cloud for maximum business value is." After 48 months of maturing, cloud efforts have delivered cost transparency and improved cloud resource management.

EXPERIENCE OF CLOUD LEADERS

5	Average years of cloud experience and leadership
100%	Those that classify themselves as cloud-first, especially for new applications
90%	Percentage of new applications effectively on cloud
5	Number of hyperscalers on which they have deployed applications
80%	Expected growth of cloud in the next 3 years

10 lessons learned from the cloud trenches

CLOUD MIGRATION PLANNING

1. Lay the groundwork for cloud acceleration by leveraging containers, automation, and SaaS
2. Architect your cloud journey with workload transformation in mind
3. Going cloud-native is a journey, not a 'Big Bang' event

APPLICATIONS AND WORKLOAD MODERNIZATION

6. Upskill and adopt DevOps across the organization to overcome continuous delivery hurdle
7. Adopt standardized technology stacks to speed up shift to cloud
8. Use a single control plane to manage multicloud environments

SECURITY AND OPERATIONAL MANAGEMENT

4. Confront the security conundrum to overcome inertia
5. Future-proof the business with the right security tools and standards-based platform

OPTIMIZING CLOUD RESOURCES

9. Improve cloud economics
10. Reality of being cloud-first is difficult, but deeper business benefits make cloud-first compelling

LESSON #1

Lay the groundwork for cloud acceleration by leveraging containers, automation, and SaaS

Get ready for faster cloud adoption

92% Cloud budgets continue to grow, with 92% of Asia/Pacific FSIs surveyed planning to increase their cloud spend in 2022 compared to 89% in 2020.[1]

85% IDC Financial Insights expects that by 2023, 85% of tier-1 and tier-2 APEJ banks will curate an infrastructure strategy by coalescing on-premises/ dedicated private clouds and multiple public clouds, along with legacy platforms.[2]

Profusion of archetypes

With regards to public cloud, different organizations will classify themselves as public-first, public-also, public-only, public best-fit, even public-last.

ONE UNDERLYING FACTOR JUMP-STARTING FASTER CLOUD ADOPTION

Accelerated digital transformation. Business agility and the need for speed from IT are the most important triggers for considering cloud. Since the start of the COVID-19 crisis, cloud has been a critical factor for financial institutions to succeed in the new normal of operations.

Industry cloud thought leadership

"Cloud success is about taking a more disciplined and automated approach. And then having the capability to build competitive services along the way."

Starting the journey right

Get cloud-ready

Moving legacy applications and workflows to cloud is dependent on the right decisions to replatform, refactor, rebuild, or retire.

Microservices and containers

By 2023, as a pillar of their IT multicloud approach, 70% of IT organizations will have implemented a strategic microservices and container strategy. The proliferation of microservices architecture will also break down applications into more efficient, deployable cloud components.[2]

Automation, self-service, provisioning

Self-service provisioning is at the heart of cloud computing. Users can select from a service catalog with minimal intervention from the cloud provider. The goal is less time provisioning infrastructure and bringing products to market faster.

Increase software as a service (SaaS)

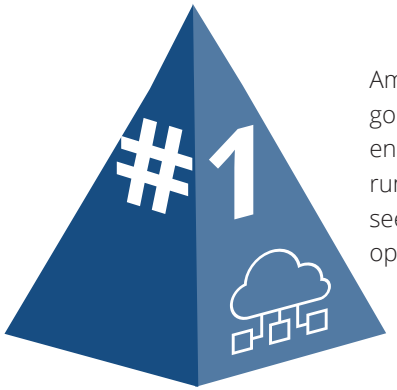
80% of businesses currently use or plan to deploy SaaS. The experience gained from SaaS will enable banks to fortify their capabilities as they adopt more cloud. SaaS is the largest and longest standing segment of cloud computing.[2]

Source:
[1] IDC Cloud Pulse Surveys (n=115, 2019 and 184, 2021 FSIs, APeJ)
[2] Cloud Outlook 2021: Cloud Is Increasingly Becoming a Primary Route for Financial Services Collaboration, Innovation, and Transformation March 2021, IDC #AP46521721

LESSON #2

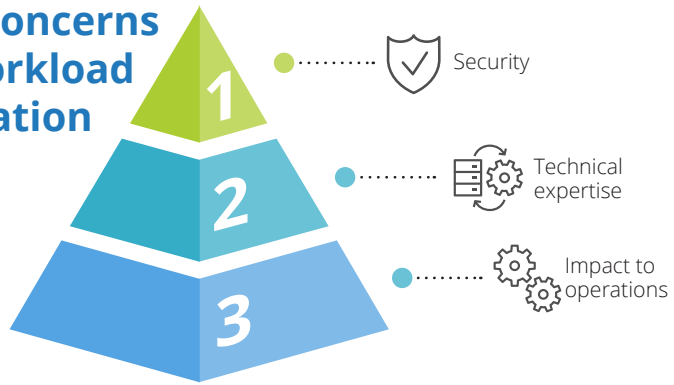
Architect your cloud journey with workload transformation in mind

#1 CONCERN FOR 2021 is workload transformation

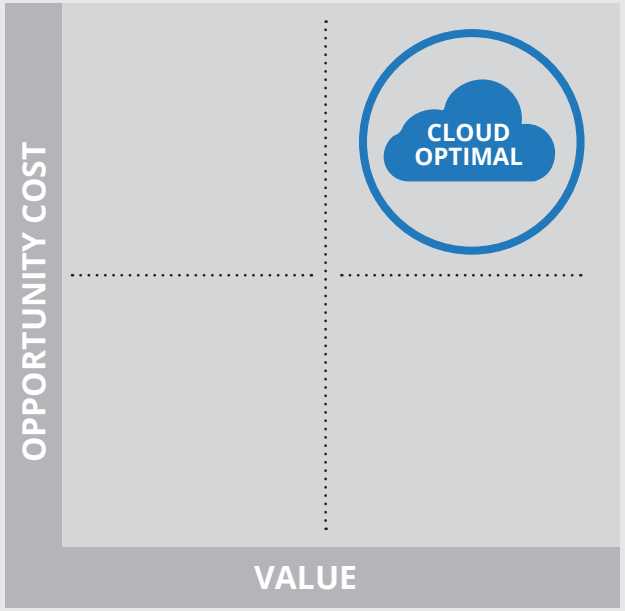


Among enterprises that have gone for a hybrid cloud strategy, ensuring that specific workloads run on the best cloud option is seen as one of the most pressing operational challenges.

Top concerns of workload migration



WORKLOADS CAN BE MAPPED AGAINST A VALUE VERSUS OPERATIONAL COST MATRIX



Industry cloud thought leadership

"We are committed to hybrid cloud. Next applications and business workflows to move to cloud will be mobile banking, loan origination, but we are evaluating more core banking on cloud."

Workload transformation essentials

Legacy systems and applications

It is difficult supporting legacy applications and systems in the long term; therefore, it is crucial to continue to modernize legacy with a view on cloud as part of the architecture of the future. In addition, legacy code is often highly inefficient, and moving to the cloud can be expensive. If legacy systems can't work on cloud, then adopting a hybrid model is the best approach. Legacy application strategies to consider: replatform, refactor, rebuild, or retire.

Cloud economics

Rethink cloud economics by reducing multicloud variability, ensuring quick business outcomes through a high degree of flexibility offered by hybrid cloud models, and considering not just the cost of moving to cloud but also the cost of ongoing operations.

Reduce complexities – simplify!

FSIs are struggling with overly complicated multicloud environments. Each additional cloud adds layers of complexity and cost. Simplify operations and drive cloud efficiency and effectiveness by having clear strategies for SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS).

Think through core application transformation

Fourth-generation core banking is cloud-native, can be configured, and allows for commercially viable licensing models encumbered by legacy core banking systems.

LESSON #3

Going cloud-native is a journey, not a 'Big Bang' event

Massive application workload modernization is underway

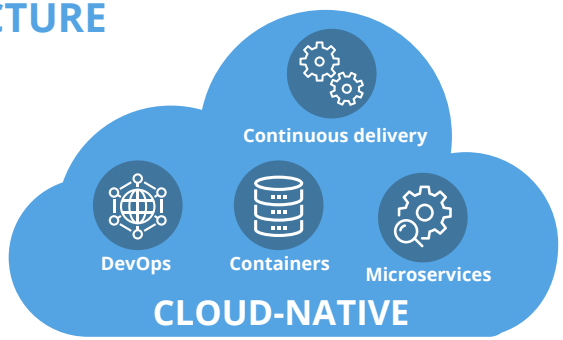
IDC's research shows a 120% growth in applications over the next two years, with 67% as the median for percentage of net new applications to be added.[1]

Adopting cloud-native core banking is also high on the agenda:

40% - 50% of APeJ FSIs are looking to change their core banking systems in the next 3 years with major considerations for cloud-native core [2]

Source:
[1] IDC Cloud Pulse Surveys (n=184, 2021 FSIs, APeJ)
[2] IDC Financial Insights Surveys

BANKS HAVE TO THINK ABOUT CLOUD-NATIVE ARCHITECTURE



Cloud-native architecture

Cloud-native means architecting your applications and future systems to take advantage of a modern cloud delivery model. Cloud-native benefits include elasticity, scale, resiliency, and leverages DevOps and continuous integration/continuous delivery (CI/CD).

Native applications and Open Source

FSIs are embracing more open-source tools and standardization, driving down costs. Enhanced cloud-native capabilities, including serverless, let you run and test dynamic workloads within milliseconds. Cloud-native applications make it easy to manage and secure applications, with maximum flexibility in pricing.

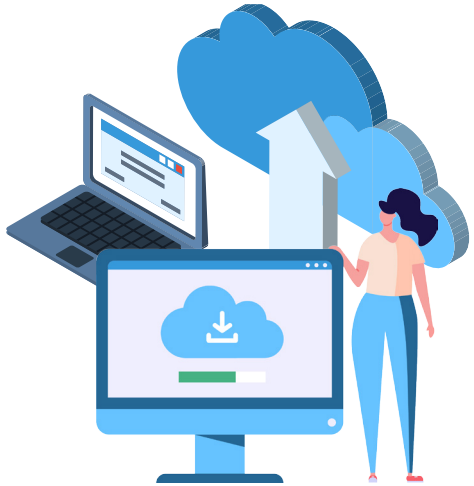
Scalability, adaptability, portability

Cloud-native reduces hardware dependencies enabling horizontal cloud scalability, helping to avoid vendor lock-in. Portability is leveraging distributed processing that pushes automation to the far edge.

Industry cloud thought leadership

"Move to cloud native because portability between on-premises and different cloud services providers is not easy."

Impact of cloud-native development



As containers start being used, these are the most likely implications to the IT organization:

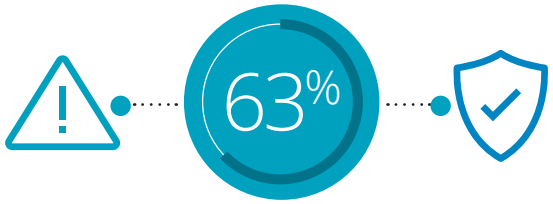
- Greater need for cloud cost management and workload assessment
- Need for better app performance and analytics tools
- Security/access control complexity

LESSON #4

Confront the security conundrum to overcome inertia

Security still a stumbling block

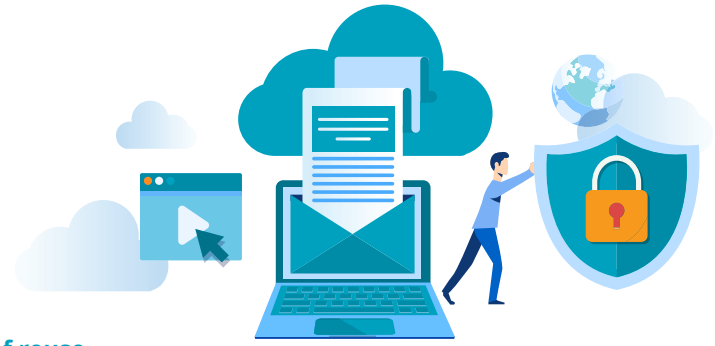
The dilemma remains around cloud for better security amid potential risks of unauthorized access.



Percentage of respondents who say that they will be spending more time in security testing – just as when they scale up cloud[1]

Key security concerns among hybrid cloud adopters

- Automated configuration, provisioning and scaling makes it too easy to insert or distribute malware and viruses
- Public cloud provider processes and tools are insufficient
- End-user password control and security diligence is lacking
- Organization lacks a cloud-first security model
- Developer security diligence as well as internal processes and tools are lacking



Lack of reuse

Most legacy security solutions don't scale to cloud. Therefore, new and different security tools must be purchased for cloud. All new FSI security platform decisions must be future-ready and cloud-scalable. Run all applications in the cloud with the same levels of controls and maturity as legacy, and at scale.

The regulators

Feedback from FSIs is that most regulators are not cloud prescriptive or directive. The same controls and rigor for on-premises computing must be applied to cloud. There are bigger challenges with having to deal with the multiplicity factors: multiple regulators, multiple jurisdictions, multiple geographies. An ongoing issue for many organizations is that customer data must stay within country.

Multiple teams, platforms, and tools

The reality is that FSIs must accept duplicity with on-premises and cloud security tools, platforms, and teams. IT organizations must skill-up to be proficient in managing new cloud security tools.

Industry cloud thought leadership

"Cloud is increasingly more secure than noncloud."

APPROACH THE DILEMMA BY RECOGNIZING THERE IS 'BEFORE CLOUD' AND 'AFTER CLOUD' SECURITY

Before cloud	After cloud
Costly, complex to manage and update	Economies of scale and full automation
Staff attrition, highly specialized skills	Leverage managed services and support
Outdated and lack of modern technology	Native, flexible, and open platforms
Legacy regulatory controls well defined and proven	New demonstratable controls and risk mitigation

Source:
[1] IDC Financial Insights Research

LESSON #5

Future-proof the business with the right security tools and standards-based platform

In the next 5 years, security will receive the highest level of investment to support cloud growth

Perceived weakness in security can blunt growth of cloud.

30%

Almost 30% of FSIs say they can backtrack from public cloud because of security concerns – the highest among all motivators for such a backtrack.

Source:
IDC Financial Insights Research

INVESTMENTS

New capabilities

Have your operational capability as a single security operation. Maximize the use of cloud-native security tools. Much more than moving your legacy world into the new cloud world, use native as much as possible. Ensure full integration, at both the security and operational level.

Need for standards

Architecture and security teams set the policies and standards. Review the output of the tools, but you need to have standardized engineering capability that's managing all aspects of security and the identity technology components.

Complexities are challenging to manage for both on-premises and cloud due to the duplication of security tools and platforms. There is very little reuse of legacy security investments for cloud, and FSIs are considering more open source solutions.

Select security solutions that will be future-ready, ensuring that the technology selected extends to the cloud.

Industry cloud thought leadership

"Difficult to leverage security tools from CSPs. Where we have selected 'best of breed' tools they are normally different from on-premises. Today costs are more but over time decommissioned on-premises reduce costs. Future is AI/ML pattern recognition tools."

MAXIMIZE MASSIVE SECURITY INVESTMENTS

- Focus on securing application workloads on the cloud and embrace cloud security shared responsibility.
- Increase velocity and scale with cloud assurance processes by creating a cloud security culture.
- Define a new cloud-optimal security operating model, selecting centralized or federated security functions.

LESSON #6

Upskill and adopt DevOps across the organization to overcome continuous delivery hurdle

Skills needed to succeed in cloud

The number of service providers to support FSIs' increased adoption is expected to jump from 18 to 21, driving up the need for more skills

>50% **of FSIs are growing staff by at least half the growth of their workloads**

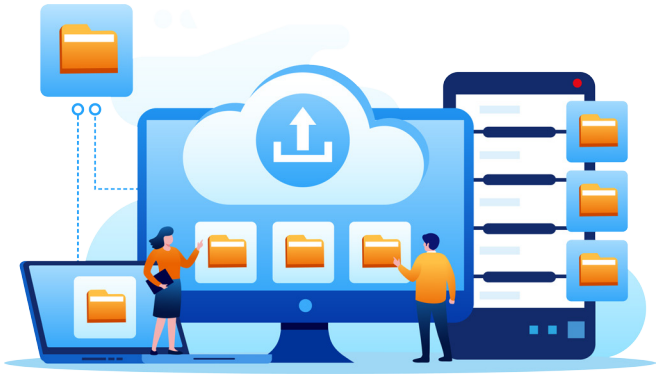
NEW SKILLS FOR CLOUD READINESS

- Cloud solutions architects
- Certified cloud security specialists
- Cloud-native software developers
- Intelligent automation, AI, ML
- Cloud Center of Excellence (COE)
- Cloud leadership and operations

Source:
IDC Financial Insights Research

Agile everywhere

FSIs demonstrate real value when operational linkages are created between all aspects of cloud, development, security, delivery, and operations. Progress is made when FSIs implement small, successive actions throughout the continuous delivery process, and later optimize and adjust to improve momentum and speed.



FSIs slow to incorporate DevOps

Many Asia/Pacific FSIs are slow to move to DevOps. This hesitation directly affects the speed, communication, and effectiveness to deliver cloud. The problem is that if there is no linkage between agile, development, and operations, cloud delivery will be compromised. The most successful organizations require new lines of reporting and different people leading the Agile and DevOps (A.DO) teams.

Evolve continuous integration/continuous delivery (CI/CD) for cloud

The endgame of A.DO is to automate, optimize, and ensure high-quality throughout the entire continuous delivery pipeline. Cloud environments benefit from DevOps with enhanced centralization of teams, with improved collaboration platforms and tools.

Industry cloud thought leadership

"Today, agile is everywhere, our new norm is agile governance. We have not combined DevOps, but we do put security by design in all stages. Embedded testing for security and dynamic security testing to include in the processes of developing new features."

DEVOPS TO DRIVE COLLABORATION AND FOR CONTINUOUS IMPROVEMENT

True cloud security shifting-left requires a change from early stages of planning, development, testing, and deployment.

Move teams to DevSecOps and leverage fully automated CI/CD and provisioning capabilities to address resourcing gaps, an escalating challenge not only in banking but across industries. About 30% of Asia/Pacific organizations suffer from a lack of skills to ensure reliable and secure digital services.[2]

LESSON #7

Adopt standardized technology stacks to speed up shift to cloud

The big shift

60%

More than half of Asia/Pacific FSIs surveyed intend to move their workloads to cloud in the next 12 months, with **more than 60% of their workloads "definitely" making that shift**

Source:
IDC Cloud Pulse Surveys (n=184, 2021 FSIs, APeJ)

Dynamics of the tech stack

The cloud technology stack represents an evolution of existing computing capabilities, advancing from virtualization, services, integration, and data center. The demands are dynamic and provide intended outcomes for what, how, and when the cloud provides services for FSIs.

Standardization benefits

Cloud is an ecosystem, not just a singular product or third-party solutions. Technical requirements drive standards to meet customers' needs. Benefits of standards include scalability, adaptability, extensibility, and manageability. However, all these should not compromise architecture, security, governance, cost, real-time availability, and performance.

On-demand services

On-demand services enable FSIs to deploy cloud components that transition beyond traditional physical resources, servers, storage, and networks. Cloud service providers manage, deploy, and deliver at scale. These new services are dynamic and enable scalability through automated provisioning of compute resources.

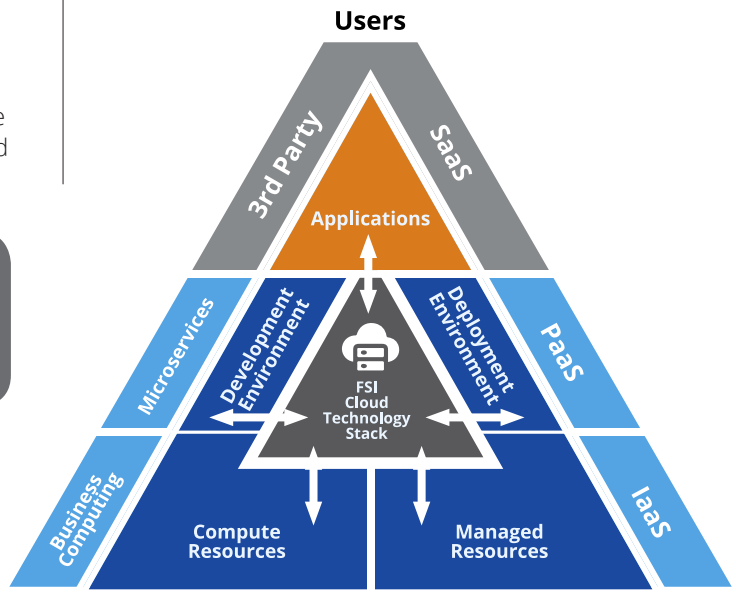
Industry cloud thought leadership

"We have built an API-centric capability to make it flexible to connect with partners, platforms, and applications. We are moving our architecture to be more microservices-based in the future."

WHAT A STANDARDIZED TECHNOLOGY STACK CAN DO

An effective standardized cloud technology stack comprises multiple layers of tools, capabilities, and services.

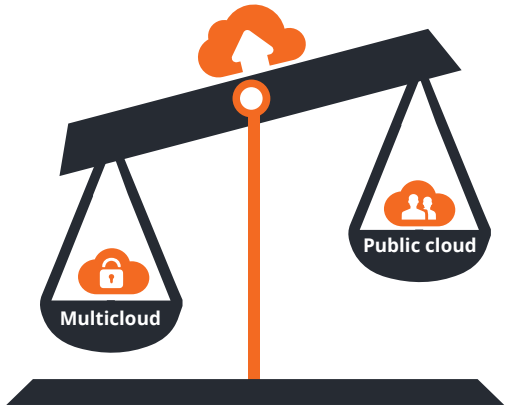
The stack must deliver real-time connectivity, data, and workflows while ensuring that the standards are inclusive of cloud architecture, security, governance, and performance.



Source: IDC FInancial Insights, 2021

LESSON #8

Use a single control plane to manage multicloud environments



Open multicloud wins over single public cloud
FSIs are increasingly working toward "real connectivity" instead of cross-cloud interconnectivity.

REAL-WORLD OPEN MULTICLOUD MEANS THIS...

- Multiple cloud environments to migrate data and workloads in between
- With single application that can run seamlessly across different clouds
- Managed using a common set of tools and processes to support seamless application operation

Source:
IDC Financial Insights Research

Singular cross-cloud control planes
Multicloud creates new complexities in operational management, and with the addition of cloud-native applications, the need for cross-cloud planes has never been greater. FSI cloud workloads will become more portable as the infrastructure becomes more ephemeral, giving way to new operational challenges.

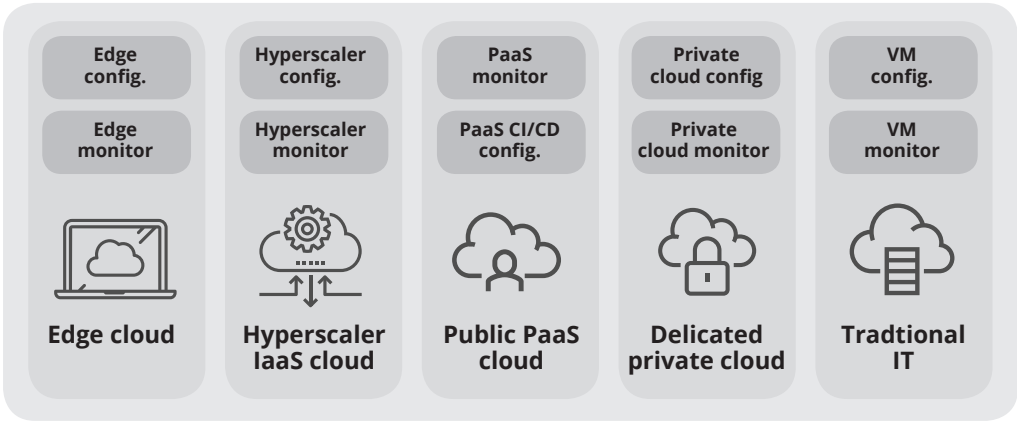
Lack of integration and automation
CIOs are still dissatisfied with the lack of integration and automation across multiclouds. The constant need for visibility, analytics, and the promise of a "single pane of glass" is not a current reality.

Provisioning and cost optimization
Provisioning and automation are necessary to support new workloads, self-service capabilities, and the dynamic nature of cloud operational management. Cost optimization depends on cross-cloud analytics to drive automation. Application and service performance requires continuous assessment at scale and at the speed of cloud usage.

Industry cloud thought leadership
"Understand the assumptions being made for cloud workloads and how resources are managed and consumed. Cloud management tools can provide indications and recommendations on when to scale back, but IT operations teams, together with the business teams, must still make the final decision."

ENSURING REAL-WORLD CLOUD CONNECTIVITY

IDC multicloud management and provisioning



IDC research: Shared cross-cloud management control planes, automated governance, and end-to-end observability are enabling connected cloud architectures to overcome many challenges encountered in older hybrid and multicloud environments. Connected cloud architectures depend on establishing a consistent open API-driven management layer to unify cross-cloud operations.

Interconnectivity through:

- Cross-cloud control planes
- Infra as code automation
- Deploying the same DevOps platform and CI/CD workflow engine
- Role-based automated development infrastructure with self-service provisioning
- Predictive AI to optimize applications performance

LESSON #9

Improve cloud economics

Overspending is a growing issue

30%

A majority of FSIs acknowledge overspending by at least 30%

WHAT TYPICALLY MAKES UP THE OVERSPENDING BILL

- Overspending typically seen in private cloud and SaaS
- Overspending on networking devices and hardware, public cloud specialized services workloads (AI/ML)

Source:
IDC Financial Insights Research

Strategic procurement

Cloud procurement is fundamentally different from traditional models for on-premises purchases, which have a high degree of customization and can be difficult to standardize. Most cloud services eliminate the need for physical assets and shift toward on-demand utility-style computing. Strategic cloud procurement focuses on performance-based requirements that prioritize applications and workloads based on business outcomes.

Active cloud resource monitoring

It can be challenging to take full costing advantage of vendor-integrated cloud monitoring tools. Many FSIs select best-of-breed cloud tools that are very different from traditional on-premises resource monitoring tools. Initial cloud costs can be high, but total cloud costs should reduce over time, based on decommissioning legacy systems and taking advantage of cloud economies of scale.

Cloud utility pricing models

FSIs must move beyond fixed-priced procurement to realize the maximum value. New models should adjust for fluctuating demand and provisioned cloud services based on active consumption. Pay-as-you-go or pay-per-use utility models are the future where organizations pay only for usage consumed at the end of each billing period.

Industry cloud thought leadership

"It takes time and resources to fully optimize the bank's cloud environment. We have a commercial team that monitors all cloud usage and leverages a leading cloud cost management platform for cloud billing and transparency."

FOCUS ON UTILIZATION

Utilization rates are ultimately a source of good ROI.

Utilization rates of cloud, especially among early adopters, are close to 100%. Among FSIs in general, utilization rates are at 65% — still same as non-cloud.

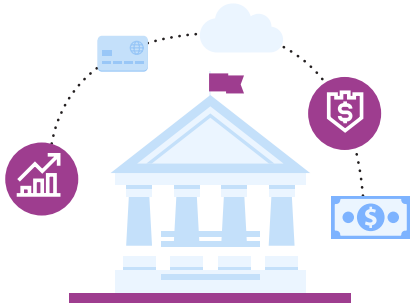
- The new paradigm of cloud economics is the discipline of minimizing the total cost of all provisioned and consumed cloud services. Cloud economics is paying for actual and active consumption versus traditional on-premises fixed costing models.
- Cloud-based resource consumption billing requires continuously monitoring cloud resources. Therefore, new cloud operational monitoring tools are necessary. Scanning and resizing resources on demand is the new challenge, as institutions only pay for the cloud services that they consume.

LESSON #10

Reality of being cloud-first is difficult, but deeper business benefits make cloud-first compelling

Strategically cloud-first, like the disruptors

Even big FSIs (not necessarily industry cloud leaders interviewed for this research piece) have committed to leverage cloud as a strategic imperative.



Challenger banks, neo-banks are 100% cloud from inception

Fintechs influencing traditional bank strategy

Source:
IDC Financial Insights Research

Going all cloud

Most FSIs are committed to going 100% cloud. However, challenges exist when replacing on-premises systems with cloud technologies. Due to complexities, the benefits do not always translate directly to reduced risk and cost.

Size and speed

Challenger banks and neo-banks have the advantage of starting with green-field cloud implementations. Smaller FSIs are more likely to be ready to move everything to the cloud faster than legacy-intensive organizations.

New products — cloud-first

New products, services, and cloud applications accessible from mobile devices facilitate going directly to cloud. Such cloud agility is vital to compete for new customers and drive attractive revenue and cost benefits. But cloud-first does not mean cloud-only; many factors, complexities, and business considerations must be factored before going cloud-first.

Industry cloud thought leadership

"Cloud is not an optional business capability; it is a necessity. CIOs must educate their boards and have engaging conversations with their senior executives on the strategic value of cloud".

LET BUSINESS JUSTIFICATION DRIVE PUSH FOR ACCELERATED CLOUD ADOPTION

- **BENEFITS** of cloud are now business growth-oriented
- ROI for cloud are now being reported at the business level showing track and report and chargeback/showback
- More than half of FSIs already report cloud metrics at a business unit or department level

IDC Essential Guidance

1. The pace of cloud adoption is now clearly determined by the institution's business goals. The direction is also **clearly toward hybrid cloud** that ensures flexibility, operational efficiency, and business agility.

2. Hybrid cloud strategies are driving toward the **ideal of interoperability** so that applications and workloads can seamlessly work through various environments.

3. **Standardization** through containers, automation, and SaaS propels the institution to quickly take advantage of the benefits of hybrid cloud.

4. Financial institutions' portfolios of applications are being quickly **built on cloud-native architectures**, which enable horizontal cloud scalability, helping to avoid vendor lock-in and leverages portability and distributed processing to extend automation to the far edge.

5. There is now a clear **distinction between the pre- and post-cloud world of IT** that is driving institutions to embrace the future of workload management, security, and application-led innovation.

IDC Asia/Pacific
83 Clemenceau Ave
UE Square #17-01
Singapore 239920
T 65.6226.0330

idc.com

@idc

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

Permissions: External Publication of IDC Information and Data

Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason. Email: ap_permissions@idc.com

IDC Doc #AP241258IB