Cloud in Financial Services

Lessons learned from 1,000 cloud projects conducted by Reply with financial institutions and a survey covering more than 100 financial institutions in the EU and the UK

REPLY

October 2021

Contents

Foreword	3
Acknowledgments	4
Authors	5
Introduction	**6**
Section 1 – Cloud Adoption in Financial Services: Where are we today?	**8**
The Rate of Cloud Adoption	9
The Future is Cloud	9
Strategic Challenges Remain	13
Section 2 – Cloud Deployment and Service Models	**15**
Overview of key Concepts	16
The Case for Multi-Cloud	19
Key Leadership Questions on Cloud Deployment and Service Models	21
Section 3 – Cloud Architecture	**22**
Different Data Centre, Same Problems	23
Driving an Effective Cloud Architecture	24
Key Concepts Underpinning Cloud-Native Applications	25
Key Leadership Questions on Cloud Architecture	27
Section 4 – Cloud Governance	**28**
What is Cloud Governance?	29
Cloud Governance Maturity in Financial Services	29
Adaptive Cloud Governance Framework	32
Key Leadership Questions on Cloud Governance	33
Section 5 - People and Culture	**34**
Lack of Cloud Expertise or Cultural Readiness	35
The People Challenge in the IT Department	37
Culture and Ways of Working.	38
Leading the Transition to the Cloud	39
Key Leadership Questions on People and Culture	41
Section 6 – Cloud Security	**42**
Cloud Security and the 'Shared Responsibility Model'	43
The Cloud Security Paradox	45
The Enablers of a Strong Cloud Security Posture	46
Key Leadership Questions on Cloud Security	50
Section 7 – Cloud Regulation	**51**
Regulatory and Compliance Concerns: The Number One Challenge	53
Operational Resilience	54
Key Leadership Questions on Regulation and Compliance	55
Section 8 – Data Management, Governance and Integration	**56**
The Cloud and the Dynamics of Data Management	57
Data Governance	58
Data Integration	60
Key Leadership Questions on Data Management, Governance and Integration	61
Section 9 – Journey to the Cloud	**62**
The Challenge of Technology Adoption	63
What is Full Cloud?	64
Different Journeys to the Cloud	65
Key Leadership Questions on the Journey to the Cloud	66
Section 10 – Leveraging the Cloud to Fuel Innovation	67
Approaches to Innovation on the Cloud	68
Experimentation and the Cloud	69
Business Model Innovation	70
Key Leadership Questions on Leveraging the Cloud to Fuel Innovation	71
Section 11 – Future Issues	72
The Green Cloud	73
Cloud-based Quantum Computing	75
Conclusion	**77**

Foreword

In recent years, cloud computing has grown from a concept to a genuine core component of business. It is increasingly clear that this is just the beginning: the services and virtual environments associated with the cloud have effectively transformed the traditional uses of technology.

The cloud is the global platform every new digital business is built upon. At Reply, we view our work in cloud as a representation of our broader support to digitalise businesses and create continuous product innovation for our clients. As CEO of the Reply Group, I seek to transmit this business philosophy in all that we do.

The authors of this publication personify Reply and this business philosophy to a tee. Our foundation of experts and forward thinkers is one of the keys to delivering change for our clients. As a pan-European leader of our financial services practice, and co-author of this piece, Freddy Gielen knows the pulse of the industry and comes equipped with the business savvy and innovative mindset necessary to recognise how technology can best serve our clients. Likewise, we believe in the importance of growing our international network of collaborations and partnerships, including arrangements with top-notch universities. As a professor at University of California, Santa Barbara, and co-author of this piece, Professor Nelson Phillips provides invaluable perspective thanks to his expertise in innovative decision making, business management, and executive education. Furthermore, I wish to extend a special thanks to all of the contributors who have brought this publication to life.

This publication channels excellent insight not just from the Reply network but provides feedback from top management and decision makers of some of the most renowned financial institutions in the world. You will get a clear and concise representation of the real challenges and opportunities that organisations face in today's information age. In fact, harnessing technology such as cloud is not just about IT solutions, but about the essential elements of all successful businesses, such as strategy, governance, and of course the bottom line. You will find that this piece covers complex technical arguments in an informative and straightforward fashion.

So, with this, I am pleased to present you the culmination (to date!) of our hard work. I hope you will enjoy this read and wish you success on your way to the cloud.

Tatiana Rizzante
Group CEO
Reply

Acknowledgments

We are indebted to a long list of industry experts and colleagues who have generously volunteered their time and experience in helping us shape this report.

In particular, we would be remiss if we did not acknowledge the following individuals who generously shared their ideas, insights and thoughts: **Arnaud Denis**, MeDirect Bank, Malta; **Adel Awad**, Arab Bank, Jordan; **Alan Clacher**, Saudi Transformation Programme, Saudi Arabia; **Alexandra Maniati**, European Banking Federation (EBF), Belgium; **Andrea Monti**, PayPal, Luxembourg; **Chris Portelli**, MeDirect Bank, Malta; **Daniele Tonella**, Unicredit, Italy; **Eric Goris**, Ethias, Belgium; **Eric Modave**, Arab Bank, Jordan; **Faycal Sbai**, BNP Paribas Cardif, Belgium & Netherlands; **Frédéric Mouchel**, Royal Bank of Canada (RBC) Investor & Treasury Services, Luxembourg; **Hans van der Waal**, Travelex, Netherlands; **Hugues Tallier**, DWS Group, Switzerland; **Huw van Steenis**, UBS, Switzerland; **Ian Haynes**, HSBC, UK; **James Saull**, AWS, UK; **Jean-Michel Hermange**, BNP Paribas Cardif, Belgium & Netherlands; **Jelena Zelenovic**, European Investment Bank, Luxembourg; **Jeremy Arnold**, NatWest Markets, UK; **Joerg Guenther**, Citi, UK; **Josip Kovacevic**, PayPal, United States; **Julian Schmücker**, EBF, Belgium; **Katty Conrard**, RBC Investor & Treasury Services, Luxembourg; **Laurent Stalens**, NRB, Belgium; **Michael McGovern**, Brown Brothers Harriman, United States; **Nathalie Charpentier**, BNP Paribas Fortis, Belgium; **Oleg Lebedev**, PRMIA, UK; **Patrick Devis**, Belfius, Belgium; **Peter Wintsch**, Pictet Group, Switzerland; **Roman Koch**, Baufinex, Germany; **Ross Gardner**, Royal Bank of Canada, UK; **William Poos**, NRB, Belgium.

We are also indebted to the cloud experts at Reply with whom we discussed the many issues that are reflected upon here: **Andy James**, Cluster Reply, UK; **Baxter Willis**, WM Reply, UK; **Ben Walker**, Airwalk Reply, UK; **Dan Dawson**, Go Reply, UK; **Didier Palut**, Data Reply, France; **Electra Panagiotopoulou**, Glue Reply, UK; **Filippo Rizzante**, Reply, Italy; **Hans-Peter Sailer**, Machine Learning Reply, Germany; **Jason Hill**, Reply, UK; **John Sidhu**, Glue Reply, UK; **Karine Marechal**, e*Finance Consulting Reply, UK; **Luca Gardini**, Go Reply, Italy; **Luca Mayer**, Spike Reply, Italy; **Marco Noli**, Reply, UK & France; **Martin James**, Mansion House Consulting Reply, UK; **Matt Mould**, Storm Reply, UK; **Mike Ellerton**, Go Reply, UK; **Paolo Fabris, Avantage** Reply, Italy; **Russel Ahchow**, Glue Reply, UK; and **Tim Falla**, Glue Reply, UK.

We owe a particular word of thanks to members of Reply's financial services Senior Advisory panel, including **Frédéric Mouchel, John Finch, Mark Clatworthy**, and **Yves Dermaux**, who helped us get to the core of the matter on many of the issues discussed in this report. Their insights as former global executives and independent non-executive directors in global financial institutions helped us evaluate some of the most intricate technological issues from a strategic perspective.

Finally, we would like to give a big thank you to the team at Reply and Imperial College Business School who lived this report with us for many months, discussing every idea and contributing in so many ways. They helped shape both this report and the underlying survey, and we could not have done it without them: **Aaron Miani**, Reply, UK; **Catherine Whitecourt**, Go Reply, UK; **Chris Rossi**, Avantage Reply, Italy; **Cleo Silvestri**, Imperial College Business School, UK; and **Professor Markus Perkmann**, Imperial College Business School, UK.

We are deeply grateful to all those who helped us with this report and the survey. However, the views and opinions expressed are strictly those of the authors and do not necessarily reflect the views of those who contributed or the position of their employers.

Authors

Freddy Gielen,
Reply

As Executive Partner, Freddy is focused on enabling change within Reply's financial services clients by leveraging the firm's strong technology and innovation DNA and deep financial services industry experience.

Freddy previously served as Partner for Avantage Reply, a pan-European risk and regulatory management consultancy he had co-founded in 2006. Under his leadership and that of his co-founders, Avantage Reply grew from a four-person London-based consultancy to an internationally recognised firm, before it was acquired by Reply in 2011. Freddy still assumes responsibility for Avantage Reply's seven offices across the European Union and the UK.

Prior to founding Avantage Reply, Freddy spent five years at the World Bank Group in Washington, DC, focusing on financial sector regulation. Earlier in his career, he worked as a senior manager with Ernst & Young in San Francisco and Asia Pacific. He started his career with Arthur Andersen.

Professor Nelson Phillips,
Professor of Technology Management,
University of California, Santa Barbara

Nelson Phillips is Professor of Technology Management at the University of California, Santa Barbara. Until recently, he was Professor of Innovation and Strategy and Co-Director of the Centre for Responsible Leadership at Imperial College Business School. Professor Phillips' research interests cut across strategy, innovation, and leadership and he has a particular interest in what happens where digital technology and people come together. In addition to his research, he is currently the co-editor of Innovation: Management & Organisation, sits on the board of governors of the Academy of Management, and is a trustee of the Society for the Advancement of Management Studies.

Professor Phillips teaches leadership, strategy and digital business, as well as delivering executive education programmes for a wide range of corporate clients including the London Stock Exchange, Savills, Barclays, ASDA, Panasonic, the NHS and Edwardian Hotels.

Introduction

> "Today the key competitive advantage in financial services is how firms – and supervisors – collect, store and analyse the explosion of data. Just as the steam engine transformed manufacturing, AI, ML and cloud-based technologies are transforming services."
>
> **Mark Carney, then Governor of the Bank of England, June 2019**

One dramatic impact of the coronavirus pandemic has been the rapid acceleration in the digital transformation of organisations as much of the workforce has been suddenly forced to work from home.

The ability of organisations to close physical offices and continue operating rested largely on various kinds of cloud services providing distributed, on-demand availability of data storage and computing. While the move to the cloud was already well underway prior to the pandemic, what Gartner has called the growing cloud-first preference of organisations has become a cloud-only necessity. The traditional drivers of cloud adoption – reduced cost, rapid ability to scale and global reach – have become secondary to the new necessity of virtual organising.

One industry where cloud adoption was already well underway is financial services. One of the initial challenges in approaching this hot topic is the meaning of cloud to financial institutions. While cloud can easily be seen as a technology 'project', its key value is in fact the capabilities it unlocks for the way organisations do business. The posture has changed significantly in the last few years and this technology 'project' perspective has largely subsided in most industries. It is interesting to note that though the financial services industry has long been a laggard in this respect, often held back by regulatory considerations and organisational challenges, most financial institutions now see the cloud as a fundamental pillar of their business strategy.

This unlocking of capabilities is focused on aspects such as flexibility, agility, time to market and delivering digital capabilities in line with customers' and employees' increasingly demanding always-on expectations. As such the cloud is a key enabler that supports business change and transformation.

This report outlines insights into the use of the cloud across the financial services industry. It presents an observatory of trends and developments on the use of the cloud in 2020/2021 and provides financial institutions with ideas and insights to help them address important questions as they move more and more activity to the cloud.

We have divided this report into multiple sections, covering the key areas that underpin successful cloud adoption. Our conclusions have been informed by the work Reply has performed since 2009 across circa 5,000 cloud projects, of which more than 1,000 are in financial services. This body of empirical knowledge is supplemented by more than 30 interviews with senior leaders in financial services conducted between May 2020 and January 2021 and by a survey of 277 (primarily UK- and EU-based) financial services professionals from November 2020 to February 2021, under the methodological direction of Imperial College Business School professors.

Section 1

Cloud Adoption in Financial Services: Where are we today?

> "Our collective experience with the pandemic has probably provided proof to the assertion that we made in 2019 in *The Future of Finance Review.* We asserted that the cloud has matured to the point where it is resilient, commercially viable, and very appealing for both traditional and new financial institutions. The last 18 months has been a proof point for the maturity achieved by cloud technologies and made Board Members and the C-Suite increasingly aware of how beholden they are to the cloud."
>
> **Huw Van Steenis, Group Managing Director and Senior Advisor to the CEO, UBS (formerly, Chair of the Future of Finance Review commissioned by the Governor of the Bank of England), April 2021**

"The Bank [of England] should embrace cloud technologies, which have matured to the point they can meet the high expectations of regulators and financial services."[1] In his report (June 2019) commissioned by Mark Carney (the then Governor of the Bank of England), Huw van Steenis articulated the extent to which the UK financial system was already highly reliant on the cloud. In our opinion, that is increasingly true not only for UK banks but for all types of financial institutions across the European Union (EU) and the United Kingdom (UK), which are the primary focus of this report.

The Rate of Cloud Adoption

Looking forward, while we expect a significant increase in the workloads financial institutions host globally on the cloud, we believe that the pace and the degree of adoption as well as the strategic approach to embracing the cloud will continue to vary greatly in financial services based on four key factors:

Firstly, the pace and the degree of adoption **vary geographically**. For example, the UK's regulatory stance is more cloud friendly than, say, that of some countries in the Middle East, so location significantly impacts ability to adopt the cloud.

The second factor is defined by the **sub-segments of the financial industry.** Asset management firms or hedge funds, for example, generally find it easier to adopt the cloud than those in wealth management, where there are stronger concerns about data privacy.

Thirdly, **traditional** financial institutions will naturally approach the cloud differently to **new financial institutions** that were built in the cloud from the very beginning.

Finally, **idiosyncratic factors** also have an influence. Although two financial institutions may both say they have adopted cloud technology, one may have done so only for development and testing while the other may have migrated critical applications to the cloud.

The Future is Cloud

There is a general consensus that the move to the cloud is overwhelmingly positive. As we conducted the research and survey underpinning this report, we heard again and again that "the future is cloud", due to increased productivity, innovation and scalability – and, at least as importantly, because moving to the cloud frees up time and energy for more strategic issues. Data storage and computing power are increasingly seen as utilities best left to specialised firms, i.e. the cloud service providers (CSPs), such as Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure.

[1] Future of Finance Review on the Outlook for the UK Financial System: What it means for the Bank of England, Huw van Steenis, June 2019, page 10.

> "The cloud counts amongst the technologies that have helped us leap forward. With the cloud we are moving directly into 'digital beyond banking' and to the 'marketplace economy'. We are embracing an ecosystem that is much more regional with digital platforms and interoperability with e-commerce, insurance, etc. The cloud is a fantastic enabler for such innovation."
>
> **Eric Modave, Chief Operating Officer, Arab Bank, September 2020**

As depicted in Figure 1, financial institutions responding to our survey identified **on-demand scalability** as the main benefit of the cloud, followed by its **ability to enable innovation** – a point underscored in the quote above by Eric Modave, Chief Operating Officer with Arab Bank, one of the largest financial institutions in the Middle East – and the fact that it **speeds up implementation.**

Percentage of Respondents who Selected this Benefit as one of the top three Benefits Presented by the Cloud

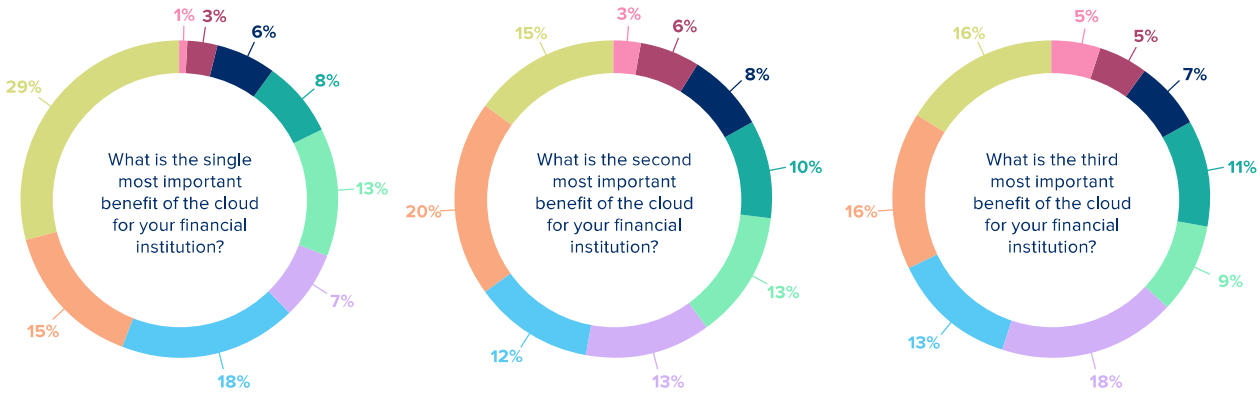


FIGURE. 1

Based on 202 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021).

We can draw at least four additional conclusions from the survey results, which are consistent with the lessons learned from Reply's cloud implementation projects in financial institutions:

- 29% of the respondents identified **on-demand scalability** as the most important benefit of the cloud; a total of 60% of the respondents view it as among the top three benefits of the cloud.
- 19% of the respondents identified **enabling innovation** as the most important benefit of the cloud; 44% believe it to be among the top three benefits of the cloud.
- Interestingly, only 7% of the respondents identified **cost savings** as the most important benefit of the cloud, although for 38% of the respondents it is among the top three benefits of the cloud. Indeed, 13% and 18% of the respondents selected cost savings as the second or third most important benefit.

  While the survey did not allow us to understand in what circumstances cost savings accrue, the interviews we conducted with senior leaders, coupled with Reply's experience within financial institutions, point to at least three important factors:

  - **Sunk costs, scale and cost savings:** Scale can be a factor and not all financial institutions will achieve cost savings resulting from economies of scale (e.g., the largest international financial institutions may find it more expensive to migrate data centres to the cloud). Existing contracts for data centres as well as capitalised hardware and software costs (collectively, 'sunk costs') typically provide a formidable dis-incentive to embrace the cloud or, for those that do migrate, a 'double whammy'. This has led some CSPs to design specific programs that package not only tools and best practices to migrate to the cloud (such as the MODFRAME approach illustrated by Matt Mould in his quote on page 12), but also financial incentives to help offset the costs associated with migrations.
  - **The maturity of the financial institution's cloud financial management capabilities**, i.e., the processes in place within the organisation to bring financial accountability to the variable cost model of the cloud. This has become a discipline in its own right, often referred to as 'FinOps', shorthand for 'cloud financial management'. Given the strategic importance of this issue, we will look specifically at this in Section 4, *Cloud Governance*.
  - Significant cost savings can be achieved when the cloud is used as an **enabler for legacy system** modernisation rather than a mere replication of the as-is (sometimes referred to as a 'lift and shift' from on premises to the cloud).

> "The primary reason for migrating to the cloud is cost and to free up time and energy for more strategic issues, rather than focusing on infrastructure. If done right, potential savings can be in excess of 50% compared to the as-is."
>
> **Global Head of Securities Services Operations & Technology, G-SIB, November 2020**

- Perhaps more surprisingly, 13% of the respondents identified removing the dependency on legacy systems as the most important benefit of the cloud and, for more than 35% of the respondents, it is amongst the top three benefits of the cloud. However, when we correlated the responses to this question with the respondents' self-assessed level of cloud knowledge (i.e., 'still learning' which accounted for 27% of the respondents, 'good understanding' which accounted for 45%, or 'expert' which accounted for 28%) it became apparent that the more experienced the respondent the less obvious the benefit was.

  This is consistent with our own experience with our financial institution clients: modernising legacy infrastructure is 'no walk in the park'. It requires a structured approach to drive decisions and break down the challenge so that the financial institution can eventually enable neo-bank (or neo-insurance, etc.) features, reduce the equivalent hardware and software costs, and remove the need for scarce legacy technology skills.

> "In recent years we have noted that our banking and insurance clients encountered major challenges as they were trying to modernise their mainframe and achieve neo-bank / neo-insurance capabilities. As an industry, we have gained in maturity and have developed tools, leveraging accelerators to break down the modernisation challenge by functionality. Storm Reply's MODFRAME is an illustration of such an accelerator when migrating to AWS."
>
> **Matt Mould, Partner, Storm Reply UK (AWS Premier Consulting Partner), April 2021**

A final point warrants attention. The Future of Finance Review recommended that the Bank of England supports financial institutions in realising the benefits of the public cloud without compromising **resilience**. For 29% of the respondents, across all levels of experience, one of the cloud's many benefits is to improve operational and cyber resilience. This needs to be balanced with the risk of (excessive) reliance on third-party suppliers (i.e., CSPs), a point of concern for many financial institutions.

> "The use of the cloud clearly brings benefits for operational resilience. But it comes with its own challenges given the limited number of CSPs. This has been recognised by the UK and European regulators who are looking at interdependencies between the use of the cloud, outsourcing and operational resilience as well as by financial institutions that are increasingly embracing a multi-cloud strategy."
>
> **Karine Maréchal, Associate Partner, e*Finance Consulting Reply UK, April 2021**

Strategic Challenges Remain

At the same time, financial institutions face a number of strategic challenges when adopting the cloud. Figure 2 depicts the primary challenges identified by respondents to the survey.

Percentage of Respondents who Selected this Challenge as one of the top three Challenges Presented by the Cloud

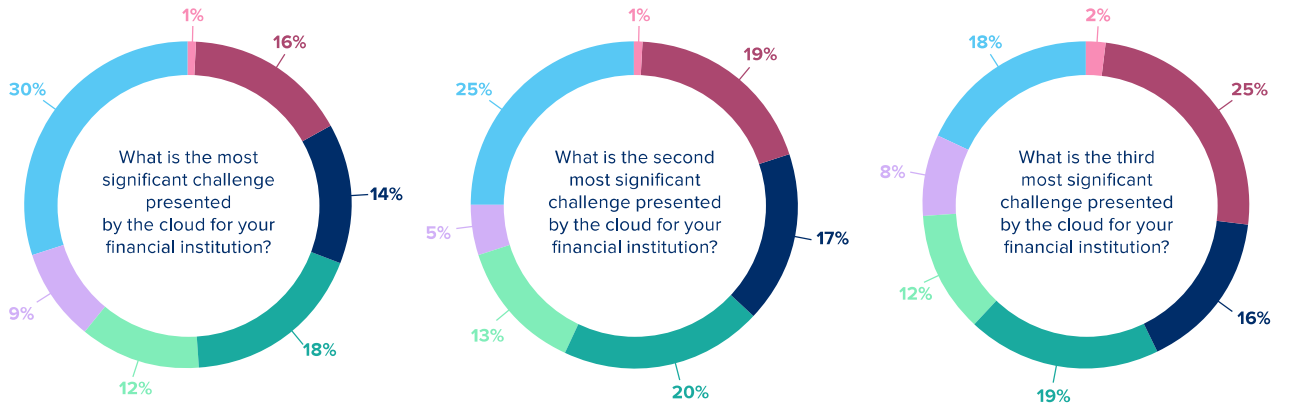


FIGURE. 2

Based on 191 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021).

Respondents singled out regulatory and compliance concerns, lack of cloud expertise or cultural readiness and security concerns as predominant challenges of migrating systems to the cloud.

Before we turn to these challenges in greater detail in the following sections, it is worth zooming in on two specific issues:

- The **incompatibility with existing systems** is an issue that was raised by a lot of respondents working in 'traditional' financial institutions. While this has most certainly been an issue in various traditional financial institutions in the past, the more recent projects conducted by Reply and our interviews with senior leaders in the industry would suggest that the issue has begun to abate.
- **Security concerns** were singled out by many respondents as one of the challenges when adopting the cloud. A number of senior leaders we talked to noted that, in the early days of the cloud, this concern often arose due to in-house IT groups (including the cyber risk teams) failing to explain the controls and level of security relating to cloud environments. Financial institutions rightly consider their client data as the 'family jewels', and therefore housing this data in a cloud environment, which they do not truly understand, is a risk they were not willing to take in the past.

This issue was compounded by the fact that the decision making for changes involving a cloud environment tended to lie with the senior leadership. Unfortunately, the lack of in-depth cloud knowledge among senior leaders in the past lead to decisions that consequently discounted cloud as a viable option.

Traditional financial institutions tend to be (extremely) risk averse and especially so when dealing with their client data. This is – in our view – one of the reasons why the adoption of cloud (which, until recently, was still regarded by many financial institutions as cutting-edge technology) was not something senior business heads wanted. As we will discuss, this has started to change and is perhaps one of the reasons why **security concerns**, while prominent in the responses, did not make it to top of the list.

Unsurprisingly, more than 74% of the respondents selected **regulatory compliance concerns** as one of the top three challenges presented by the cloud. However, when we correlated the responses to this question with the respondents' self-assessed level of cloud knowledge it became apparent that for the most experienced respondents (i.e., 'experts'), regulatory compliance – while still a concern – was less of a concern than lack of cloud expertise and cultural readiness, a point that we will revisit at length in Section 5, *People and Culture*.

In summary, cloud services are here to stay in financial services and the pandemic has only accelerated the move. But financial institutions need to be strategic in their adoption and there are important questions that need to be addressed as firms move progressively more activity to the cloud. While some of the problems are technical, there are also significant strategic and organisational challenges that need to be dealt with in the boardroom and the C-suite to ensure cloud adoption is successful and that firms derive maximum value from the move. In the following sections of this report, we will dive deeper into the most salient issues to consider.

Section 2

Cloud Deployment and Service Models

> "Cloud technology is the most important driver behind digital transformation. If done right, from enterprise architecture through security and engineering with reusable and scalable cloud native components, then time-to-market, business agility and data driven decision making will be fundamentally and drastically better than anyone could imagine when running a legacy tech estate."
>
> **Hans van der Waal, Global IT Director, Travelex, May 2021**

As noted in the previous section, there has been an unprecedented acceleration in the availability of cloud infrastructure-based solutions over the past few years. This has created an enormous opportunity to transform the way services are delivered for financial institutions, their customers, and employees. By mapping out a technology strategy for infrastructure modernisation and scalability, financial institutions can pilot their own transformation into the digital future.

At its most basic, a firm's IT infrastructure enables the execution of computation workloads that support business functions such as trading, reconciliation, treasury, credit scoring, etc. These workloads need to run and interoperate across platforms; some of which are internal to the financial institution and some that are external. Think of a shipping container network with air, road, rail, and sea – regardless of the mode, the container must move. In this section we explore the choices and considerations of the various 'transport' modes of a financial institution's 'workload containers'.

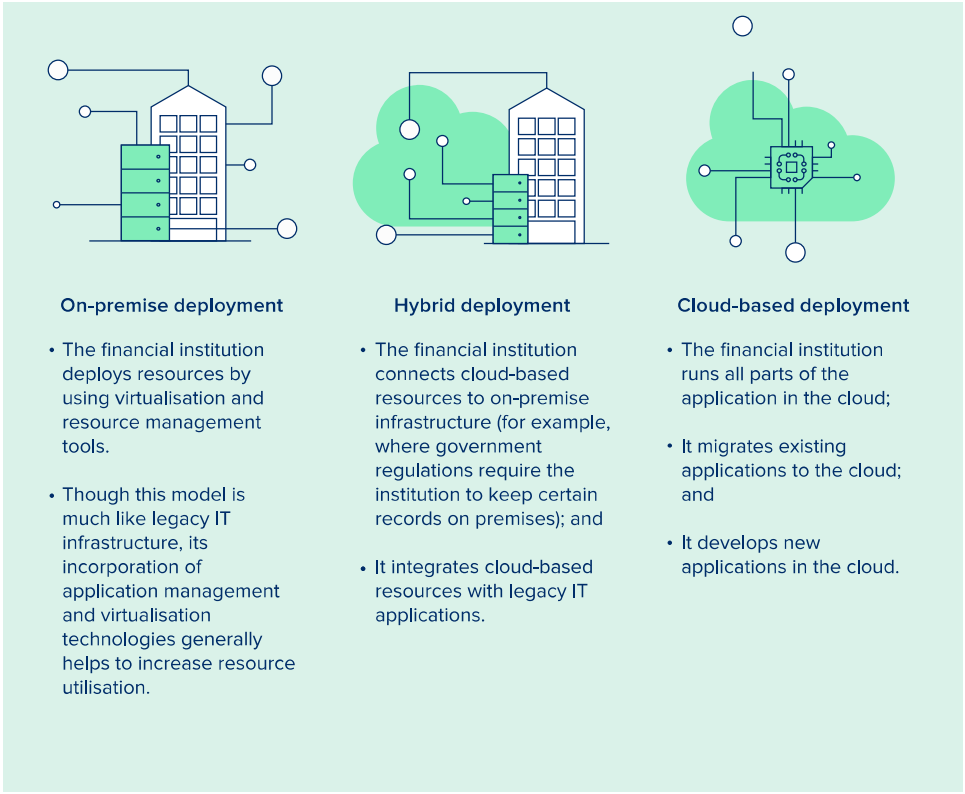
Overview of Key Concepts

Our survey respondents' answers as to why financial institutions are embracing the cloud reflect many of the usual answers – agility, scalability, cost and availability – that come with cloud-based solutions. These are easy "sells" and explain the rapid adoption of cloud in financial services. At the same time, selecting the right cloud services to achieve the predicted benefits can be a difficult proposition as cloud capabilities come in many different forms.

Introduction to Key Cloud Deployment Model Concepts

Not all IT and business solutions are created equal. Financial institutions need to have a clear deployment and service models strategy that is coherent with their strategic objectives. There cannot be a one-size-fits-all approach to cloud-based deployment and service models. When selecting cloud deployment and service models options, financial institutions must consider different scenarios against their strategic needs and, should explore tactics to improve solution performance, service cost and IT vulnerabilities. At the broadest level, there are three types of cloud service models that a financial institution may consider.

Cloud Deployment Models



On-premise deployment

- The financial institution deploys resources by using virtualisation and resource management tools.
- Though this model is much like legacy IT infrastructure, its incorporation of application management and virtualisation technologies generally helps to increase resource utilisation.

Hybrid deployment

- The financial institution connects cloud-based resources to on-premise infrastructure (for example, where government regulations require the institution to keep certain records on premises); and
- It integrates cloud-based resources with legacy IT applications.

Cloud-based deployment

- The financial institution runs all parts of the application in the cloud;
- It migrates existing applications to the cloud; and
- It develops new applications in the cloud.

FIGURE. 3

(Adapted from AWS Cloud Practitioner Essentials)

- **On-premise deployment** – In this model, also known as "private cloud", the infrastructure is privately hosted (in an organisation's data centre or a third-party data centre). The important point is that the network, hardware, services, etc. are run solely for a specific financial institution and dedicated to that organisation. This can sometimes be a stepping stone to full public cloud adoption if there is significant investment in data centres or where a high degree of control is required within the environment.

  Based on our survey, the most common perceived advantages of a private cloud are the greater security and data privacy it provides (compared to the public cloud), the greater reliability of performance and, for some respondents, a better configuration for their organisation's needs.

  However, financial institutions also highlighted a number of issues they had to address when adopting a private cloud, including the fact that it can be a more expensive solution than the public cloud and that it does not provide the same scalability.

> "We have been on a cloud mission for a number of years. We started our journey with the private cloud and are now working in partnership with public cloud service providers, ensuring that we have the flexibility to port applications from one provider to the other."
>
> **Ross Gardner, Global Head of Investor & Treasury Services Technology, Royal Bank of Canada, January 2021**

- **Hybrid deployment** – Hybrid deployment can be thought as a portion of services running in an organisation's data centre and/or private cloud, and another portion running in the public cloud. Hybrid cloud can offer cost benefits, such as where the workload and data remain relatively static and with predictable and infrequent bursts of load. In this scenario, the cloud is used for the excess workload, complementing existing investments in data centres. Naturally, some organisations may prefer to keep sensitive data on premises with other workloads on the cloud.

  Based on our survey, the most common perceived advantages of the hybrid cloud are the greater flexibility (compared to private and public cloud alone) it provides, the ability to scale to fit the organisation's needs and the greater control of security configuration.

  However, financial institutions also highlighted a number of issues they had to address when adopting the hybrid cloud, including capital expenditure requirements and complex security.

- **Cloud-based deployment** – In this model, also known as "public cloud", a cloud service provider (e.g., AWS, Google, Microsoft) make available the use of shared infrastructure, including compute, storage, network resources, etc.

  Based on our survey, the most common perceived advantages of the public cloud are its scalability, the fact that it does not involve upfront capital expenditure and the broad access to cloud-based services (e.g., SaaS) it provides.

  However, financial institutions also highlighted a number of issues they had to address when adopting the public cloud, including the risk of vendor lock-in (an issue that we will revisit in Section 7, *Cloud Regulation*), cost control (see Section 4, *Cloud Governance*), and the risk of lack of end-to-end control over security (an issue that featured prominently in the concerns raised by the institutions we surveyed and is covered in Section 6, *Cloud Security*).

Introduction to key Cloud Service Model Concepts

The "public cloud" entails three main service models as depicted in Figure 4, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Senior management and board members should be familiar with these key terms and understand the benefits, costs, risks and opportunities of selecting different options:

- **IaaS** – IaaS is the computing infrastructure – physical computers and servers, networks, firewalls, routers, etc. – that carries, stores and processes data and runs systems. The key point is that a third-party (e.g., AWS, Microsoft, Google) manages the system and provides these services over the internet on-demand.
- **PaaS** – The financial institution has access to the required infrastructure capabilities (like with IaaS) – servers, storage, etc. – as well as development tools, database management systems, etc., to support the end-to-end application lifecycle (i.e., building, testing, deploying software). By removing the complexity of managing and provisioning the infrastructure, the middleware, software licenses, etc., the productivity of teams can be increased. PaaS is consumed as a service over the internet and paid for as used.
- **SaaS** – The financial institution connects to and uses cloud-based applications over the internet (or via a direct link if there is a requirement for heavy usage, high bandwidth, etc.) instead of running the application in a data centre.

Cloud Service Models

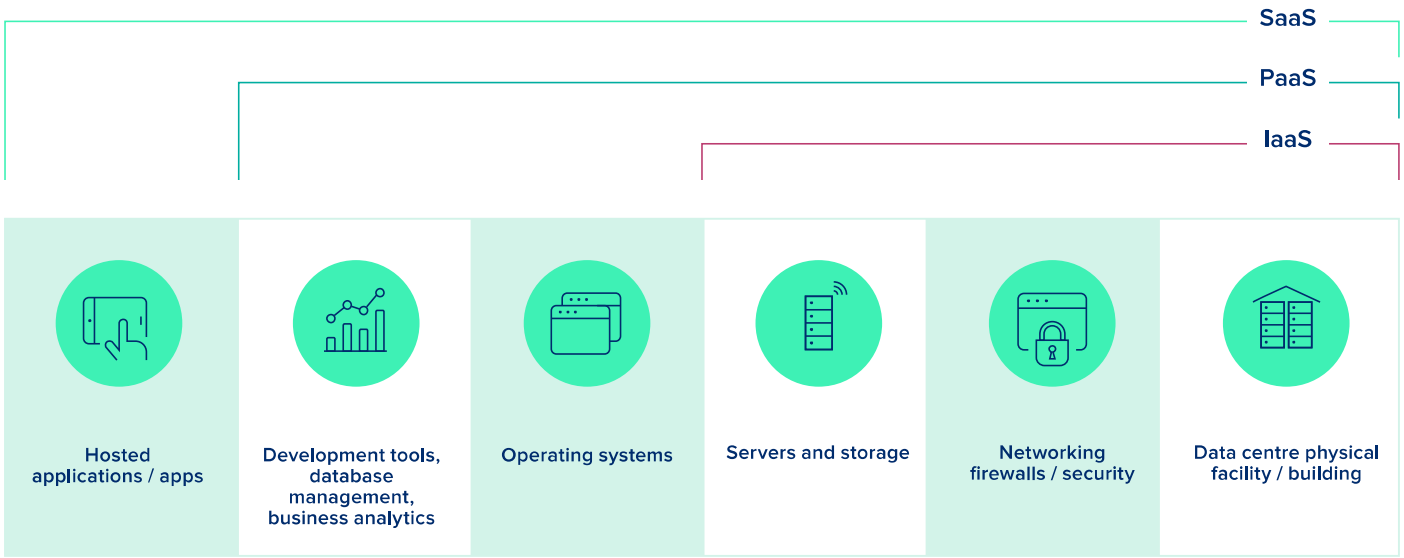


FIGURE. 4

(Adapted from Microsoft Azure Overview)

The Case for Multi-Cloud

Financial Institutions need to consider the adoption of the different models and services described above and understand the related potential advantages and issues. It is worth noting that determining whether these potential advantages and issues apply (and how to best mitigate these issues) often is a function of a financial institution's specific circumstances.

In general, the most likely outcome for financial institutions in the near future is that they will have mixed environments consisting of hybrid, public, and private clouds, and likewise a mix of IaaS, PaaS and SaaS services.

In financial services, several institutions have also considered the deliberate use of cloud services from more than one cloud service provider.

Based on our survey, the most common perceived advantages of the so-called "multi cloud deployment model" are the ability to avoid vendor lock-in as well as access to best of breed capability.

Some respondents also emphasised that it results in greater purchasing leverage and can reduce latency through geographical distribution.

The senior industry leaders we have interviewed who deployed this model noted that it also comes with challenges, including complexity, the fact that they may at times lose the innovation advantage of cloud service providers as well as more complex cost management.

In summary, each financial institution is at a different point on its journey to the cloud. The choices it makes should be dictated by the strategic objectives it is pursuing and the challenges that the institution faces. This is often complicated by legacy IT systems inhibiting change and by the fact that the cloud of today is not an end-state. Investment, industry disruption and growth opportunities continue to drive innovation. Therefore, having a well-defined cloud strategy with a robust IT infrastructure that enables flexibility, interoperability and scalability is key to the success of the organisation and must be the first step in a business's digital transformation journey.

Key Leadership Questions on Cloud Deployment and Service Models

Executives and board members should understand the implications of these mixed environments and challenge management for a coherent strategy to optimise their position, considering cost, risk, complexity, agility and innovation. Some of the questions that a financial institution may consider while developing its cloud strategy include:

Current versus target infrastructure position:

Why change the current infrastructure position? For example:

- What is the business cost (financial, opportunity, reputational) of un-planned IT outages?
- How does the organisation assess end-to-end IT security vulnerabilities in older business systems?
- Does the organisation have current benchmarks for IT service delivery?
- What is the implication of multiple in-house data centres for the organisation's green agenda?

How does the proposed cloud deployment and service models solution deliver better results from a commercial, risk and regulatory perspective? For example:

- Does legacy and data centre cost apportionment skew true business return on investment?
- What are the implications of a stressed exit?

How will the organisation ensure that the proposed cloud deployment and service models deliver benefits? For example:

- What percentage of IT service costs are running production systems? What percentage is waste? What ancillary costs can be removed (heat, light, power, building insurance, physical security, facilities maintenance)?
- What inhibitors to change can be removed from legacy IT?

Infrastructure cost considerations:

- What are the migration (and any dual running) costs involved?
- Given the on-demand nature of the public/hybrid cloud environments, how will the organisation optimise and manage cost?
- What is the marginal rate of cost increase of the infrastructure as the business scales?
- Is the shift from capital to operational expenditure an advantage and why?

Infrastructure compliance considerations:

- What are the regulatory and compliance implications of the proposed infrastructure?
- Can the future infrastructure deliver performance, availability and resilience in line with regulatory requirements and supervisory expectations?
- Does the organisation understand the disaster recovery and business continuity implications?
- Does the proposed cloud infrastructure complicate or simplify these considerations?

Section 3

Cloud Architecture

> "When moving to the cloud, you start with a single initiative, you grow and you learn. You should start small but think big and have a vision as to where you want to land."
>
> **Patrick Devis, Chief Technology Officer, Belfius, June 2020**

In this section, we will explore the need for and purpose of an architectural approach to cloud adoption. By cloud architecture, we mean the blueprint and principles that ensure the implementation of cloud services and applications will meet the financial institution's business objectives.

Many of the senior leaders we talked with while conducting the research for this report had taken a similar approach: they looked for opportunities to achieve cloud benefits, they experimented and, ultimately, they articulated a vision that served as a lodestar for their cloud strategy. Turning that vision into reality is where the need for cloud architecture becomes critical.

Different Data Centre, Same Problems

The number one problem to avoid is the 'different data centre, same problems' situation. In this scenario, the approach to cloud adoption is to replicate what is done today in existing data centres in the cloud. While this approach may seem obvious, it is fundamentally flawed and can, in fact, delay the realisation of the benefits of moving to the cloud.

The senior leaders we interviewed repeatedly emphasised this key architectural point: financial institutions need to challenge themselves to avoid using the cloud as an extended data centre. The cloud experts at Reply drew a similar conclusion from their cloud project experience since 2009, determining that a much more strategic approach is required, one that is also holistic in nature.

> "When contemplating the adoption of the cloud, an Enterprise Architecture approach that considers all the different facets required to be effective needs to be the underpinning approach."
>
> **John Sidhu, Partner, Glue Reply UK, April 2021**

Driving an Effective Cloud Architecture

In the construction industry, while the responsibilities of engineers and architects may overlap, both are integral to the design and construction of a structure. The architect designs the building to meet the client needs; the engineer's main responsibility is to ensure the design is safe and functional. This interface is equally essential to successful cloud adoption.

Cloud Enterprise Architecture

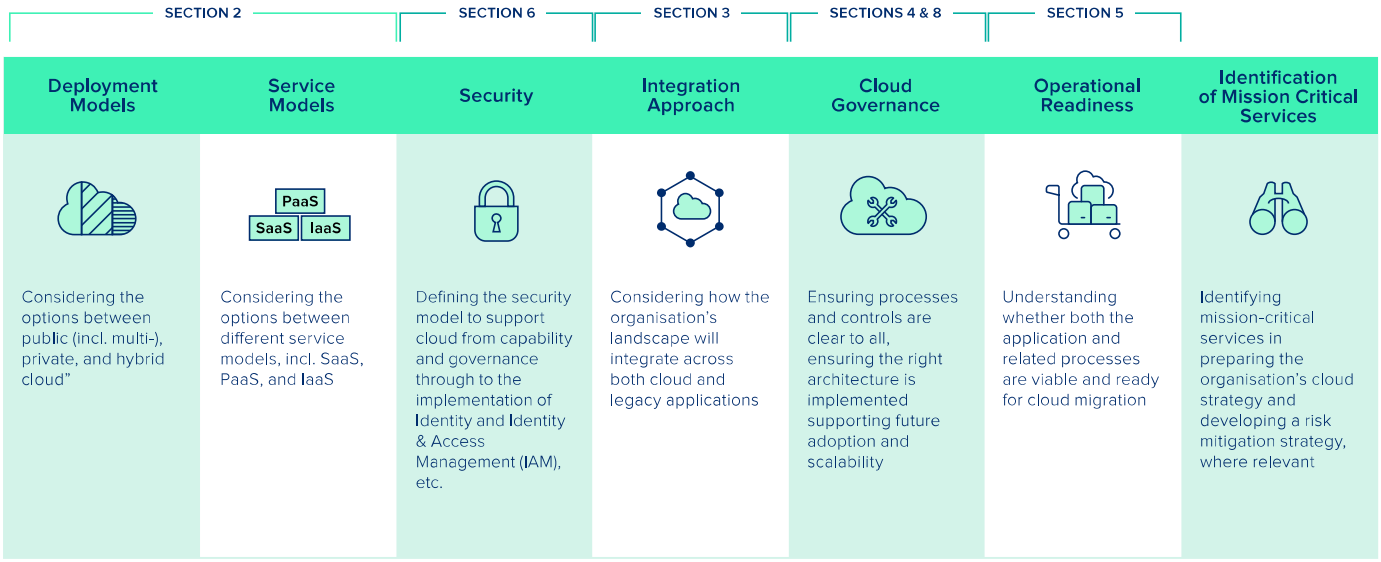


FIGURE. 5

The senior leaders interviewed pointed to seven themes to be considered when contemplating cloud adoption. Their insights enriched with the experience of Reply's cloud architecture specialists are encapsulated in Figure 5 and developed below.

- **Deployment models:** As covered in Section 2, *Cloud Deployment and Service Models*, the decision-makers must have an understanding of the public, private, hybrid, and multi-cloud options before them — and which best suits the financial institution's business requirements now and in the future.

> "When it comes to the architectural considerations, it is vital for Board members and the C-Suite to understand the key principles – not at a technical level – but in terms of business implications."
>
> **John Finch, Technology Advisor to Private Equity and Senior Advisor to Reply, May 2021**

- **Service models:** In Section 2, we also discussed three primary models. The main differentiator between them is the level of service provided to the financial institution versus the level of service it must provide for itself.
- **Security:** All survey respondents confirmed that a robust security model is critical. While many respondents noted that the capabilities of the CSPs far exceed those which can be consistently delivered in a traditional data centre, the biggest security problem in cloud adoption is that a financial institution's existing processes and controls are not well attuned to cloud and follow an older paradigm. Given its importance, this issue is further developed in Section 6 of this report.

> "What you have to do is to make sure that the way of transferring the data from where you are originating it to where it is being stored is robust; that is where you probably have the most risk of data leakage."
>
> **Jeremy Arnold, Chief Risk Officer, Natwest Markets, May 2020**

- **Integration Approach:** This is an important and complex topic because, both during and post-transition to the cloud, the financial institution will have an IT estate that includes on-premise data centres, cloud data centres and, potentially, multiple CSPs. The bridging of networks required to support this context requires thoughtful planning and diligent execution. A flexible and scalable integration approach becomes more important than ever, requiring a fundamental mind shift from the traditional approach to technology integration as part of cloud adoption. We will explore this further, introducing the concepts of microservices and APIs in the following paragraphs.
- **Governance:** As with any critical infrastructure or asset, there is an obvious need for sound governance. Aspects to consider are the holistic cloud model, appropriate controls for data, security, business process and automation. Yet there are also more operational governance considerations around managing usage, cloud financial management (or 'FinOps' as discussed above) and allowing access to services for self-serve capabilities. Given the importance of governance to the adoption and success of the cloud, this issue is further developed in Sections 4 and 8.
- **Operational Readiness:** As the context changes and the financial institution moves from data centres to the cloud, it will require new skills (e.g., DevOps, CloudOps, DataOps). The senior leaders we interviewed emphasised this point: Successful cloud adoption requires profound organisational change; we will develop this issue further in Section 5, *People and Culture*.
- **Identification of Mission Critical Services:** This is fundamental for ensuring that essential business services are operationally resilient.

Key Concepts Underpinning Cloud-Native Applications

When designing and developing new cloud-native applications, there are two critical architectural concepts to consider. These are the use of microservices and the development of application programming interfaces (APIs). These two core concepts, coupled with flexible integration points, will deliver state-of-the-art solutions that can fully harness the benefits of the cloud.

> "Microservices create ownership of products within teams that own the requirements, the delivery and operations. The cloud allows a small team to remain a small team by standing on the shoulders of giants."
>
> **James Saull, Senior Manager, Solutions Architecture – Global Financial Services, AWS, June 2020**

APIs connect the layers and components of the cloud together to make them work consistently, resiliently and at scale. In so doing, cloud native applications deliver better development productivity, improved automation and reduced time to market. They also expose the layers of the architecture to allow different components of a cloud solution to exchange information and deliver end-to-end business processes. In a cloud environment it is imperative to get the foundational concepts right first. The API and microservices ecosystem is intrinsic to this.

However, to exploit such capabilities, competencies and upskilling are required in topics such as Continuous Integration and Continuous Deployment (CI/CD), as well as new roles that enable the more rapid development of solutions. Underpinning cloud adoption is a competence development theme making the organisational capabilities cloud effective. In Section 5, *People and Culture,* we discuss how financial institutions are trying to address this significant challenge.

In summary, although the cloud has the potential to reduce cost, increase performance and enable significant business benefit, financial institutions must consider the why, what and how, so that a sound cloud blueprint can be executed. With disruptors in financial services often being new, cloud-native organisations (or at least seeking to be so), there is a strong imperative throughout the industry to create more robust capabilities, more resilient services, elastic scalability and the ability to deliver a better employee and customer experience.

Is there a pot of gold at the end of the rainbow? Our research suggests that careful consideration of architecture is key to the route to success with cloud adoption.

Key Leadership Questions on Cloud Architecture

Executives and board members should understand the implications of these architectural considerations. Some of the questions that a financial institution may ask when considering a cloud architecture strategy include:

Why move to the cloud?

- Is inflexible IT placing constraints on the business model or inhibiting business change and growth?
- Is business advantage possible through faster end-to-end information processing or more advanced data insights?
- Is reputational risk likely due to IT outages?
- Can the service cost ratio be improved with a more flexible approach to delivery?

What cloud models best serve the business objective?

- What are the security implications for data sovereignty?
- What are the considerations for concentration risk and stressed exit?
- What are the cost implications and cost benefits of the FinOps models?
- What new skills are needed to support a cloud operation?

How will the cloud architecture be realised?

- How will the organisation determine the roll-out model for cloud and workload migration?
- How will the mixed service model operate?
- How will the cloud foundations be laid?
- How will new capabilities be developed using microservices and APIs?

Section 4

Cloud Governance

> "The cloud will do to IT what Lean methodology did to manufacturing. Years ago, US companies visited Japan to learn Kaizen and Lean manufacturing. The cloud is facilitating the same level of automation in IT as Lean methodology did in manufacturing. However, the nature of managing IT at scale is managing complexity. The cloud, in its purest form, solves the dilemma of complexity provided you have a strong architectural function that ensures that different teams aren't all over the place with their own small, local complexities."
>
> **Daniele Tonella, Group CIO, Unicredit, June 2020**

Given the importance of getting the most out of the transition to the cloud, financial institutions – and, in particular, their boards and C-suite – must ask themselves three key questions:

- How does our company structure its organisational processes and governance?
- Which metrics do we use?
- How should we organise the parts of the organisation which are traditionally centred around manual processes when they can now be automated?

What is Cloud Governance?

Forrester defines governance as *"the ability to provide strategic direction, track performance, allocate resources, and make adjustments to ensure that organisational objectives are met, without breaching the parameters of risk tolerance or compliance obligations."*[2] When it comes to cloud computing in financial services, governance is the agreed-upon framework of policies and standard practices that a financial institution defines and implements to operate in the cloud in line within the parameters of its risk tolerance and in compliance with applicable regulatory requirements.

Typically, the cloud governance framework will cover a range of topics including asset management (e.g., compute or storage resources used by the financial institution), configuration management, financial management (i.e., cost control policies for all cloud platforms), cost optimisation, security, performance management, cloud operations, resiliency, and regulatory compliance (including compliance with outsourcing regulation).

Cloud Governance Maturity in Financial Services

> "Moving to the cloud is not just about lifting and shifting data and systems from on premises to the cloud. Adjusting your operating model and governance framework are key success factors."
>
> **Alan Clacher, Senior Adviser, Saudi Transformation Programme and former Head of IT RRC, Deutsche Bank, May 2021**

[2] Adapt your Governance Framework for the Cloud, Forrester Research, Dave Bartoletti, August 2018.

As depicted in Figure 6, financial institutions responding to our survey identified cloud governance as a key enabler for a successful transition to the cloud, a point underscored in the quote above by Alan Clacher, Senior Advisor to the Saudi Transformation Program and former Head of IT RRC, Deutsche Bank.

How well Developed is your Organisation's Cloud Governance?

Our cloud governance includes:

FIGURE. 6

Based on 177 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021). Respondents to the survey were asked to rate how well these various aspects of cloud governance were developed in a scale from 1 to 5.

The survey suggests that the most advanced building block of cloud governance in financial institutions is the information security framework (64% of the respondents rate it as either "adequate or "very well developed"). While this may be contrasted with the lower rating assigned to IAM and RBAC, this is nonetheless an impressive score and one that reconciles with Reply's experience. All told, this is an area of significant investment for financial institutions choosing to embrace the cloud; one where the CSPs have also invested a lot of effort.

While financial institutions will no doubt want to continue to further develop their cloud security posture, the survey highlighted three areas where there appears to be a pressing need to address governance weaknesses. This too we find to be consistent with Reply's experience and the views expressed by senior leaders interviewed. Cost management, data governance and managing the risk of outsourcing (i.e., running on the hyperscaler's infrastructure) all require focus:

- **Cost management and optimisation:** The reality of 'on demand' and quasi-infinite capacity coupled with consumption-based licensing means cost is difficult to control and is often only visible when the bill arrives. The most advanced users of cloud we interviewed emphasised the importance of embracing FinOps to address this issue.

  Almost 60% of the respondents find weaknesses in the way their organisation manages cloud expenditures, including a surprising 11% who noted that they have not cloud cost control management framework in place.

  Our interviews with senior leaders in financial institutions and Reply's experience with large financial institutions show that this challenge is compounded in organisations with large and complex cloud environments. This calls for the implementation of cost optimisation and cost management policies and budgets, all underpinned by automated tools (e.g., a tool triggering an alert when a specific department cloud spend is nearing its budget limit).

  Cloud cost analytics capabilities are becoming an essential component of any financial institution's cloud governance framework. And, as evidenced by a recent cross-sectoral survey by the FinOps Foundation,[3] financial institutions are not alone in this quest for enhanced cost management and cost optimisation capabilities. The Foundation found that only 15% of surveyed organisations have found their stride; a majority are only starting out or beginning to establish FinOps practices.

  Interestingly, the FinOps Foundation survey echoes the experiences of the Reply teams over the years: one of the biggest challenges the FinOps teams face is reducing waste or unused resources (e.g., rightsizing underutilised assets, terminating 'zombie' assets).

- **Data governance and use:** Unsurprisingly, with the dramatic increase in the volume of data generated and used by financial institutions, and with the growing number of financial institutions trying to leverage cloud capabilities for use in data science and data analytics, the senior leaders we interviewed all underlined the importance of data governance. The survey response underscored that this remains an area for improvement in most financial institutions. As we will discuss further in Section 8 the challenge is to develop and implement a framework that manages data as a strategic asset for the financial institution in a way that fuels innovation and complies with data privacy requirements.

[3] State of FinOps Report 2021, FinOps Foundation, 2021

- **Outsourcing risk:** Tellingly, there is real opportunity to better manage outsourcing risk. 60% of the respondents noted that the management of cloud outsourcing risk in their organisation requires (significant) improvement or is not developed at all.

  As with all technology and operations, the contract for service is an important element of the cloud operating model and governance. Will the service and capability do what the organisation needs, will it scale as required, and will it, ultimately, deliver value? Strong governance and vendor relationship management is required to ensure success.

  Beyond the important business and operational resiliency issues that have to be addressed when outsourcing infrastructure, application and other capabilities to CSPs, there are also regulatory concerns, as noted by the respondents and discussed in Section 7.

Adaptive Cloud Governance Framework

As noted in Section 2, the cloud of today is not an end-state – technology is in rapid and constant evolution. At the same time, business models and the external environment evolve rapidly. To ensure a financial institution can respond to these changes, an organisation's governance – and, in particular, its cloud governance framework – should be reviewed on a regular basis.

Accordingly, the capacity of the cloud governance framework to adapt to changes in the internal and external environment, as well as to the level of cloud adoption maturity of the financial institution, is particularly important.

In summary, the cloud and the capabilities and opportunities it fuels mean both the board and the C-suite must learn and learn fast. They must live with the paradox of 'leaving the teams well enough alone' while being frequently involved. They must supportively question, encourage innovative risk taking and ensure good business practice of compliance, security, privacy and sound financial management embodied by FinOps.

Key Leadership Questions on Cloud Governance

Executives and board members should understand the governance changes that the organisation should implement when transitioning to the cloud. Some of the questions that a financial institution may consider regarding its cloud governance framework include:[4]

Cost management:

- Has the organisation developed and implemented cloud cost management policies, providing for the creation of budget at the appropriate level of granularity (e.g., business, department, cost centre...), the monitoring of said budget as well as the monitoring of cost trends?
- How has the organisation implemented these policies (i.e., ensure they are embedded)? To what extent has the organisation equipped itself with automated platforms and tooling to implement its cloud cost management policies?

Cost optimisation:

- Has the organisation developed and implemented cost optimisation capabilities to optimise and reduce costs?
- How has the organisation implemented these policies? To what extent has the organisation equipped itself with cloud cost optimisation automation?

[4] Questions pertaining to (a) data governance, (b) outsourcing risk, (c) identity and access management, and (d) network and security controls are set out in Sections 8 (for a), 7 (for b), and 6 (for c and d) of this report.

Section 5

People and Culture

> "It is very easy to do a few pilots with the cloud; it is an entirely different thing to do meaningful projects at scale. You need to take all the stakeholder groups on a journey with you, including the business, the technology organisation, the executive leadership, the bank's risk stewards, and our regulators."
>
> Ian Haynes, Head of Cloud Services, HSBC, October 2020

Successful cloud adoption requires profound organisational change. As a result, it is as much about people as it is about technology. In fact, both the speed and impact of cloud adoption are highly dependent upon the availability of the right people, the existence of the right culture, and the readiness of leaders (see the *Cloud Adoption Triangle* shown below in Figure 7). Getting the technology right without having the right people, culture and leadership in place will not result in the business impact and return on investment that is possible from a well-managed transition to the cloud. Therefore, plans for cloud implementation must include a clear strategy for the soft aspects of the journey to the cloud if it is to be successful.

The Cloud Adoption Triangle

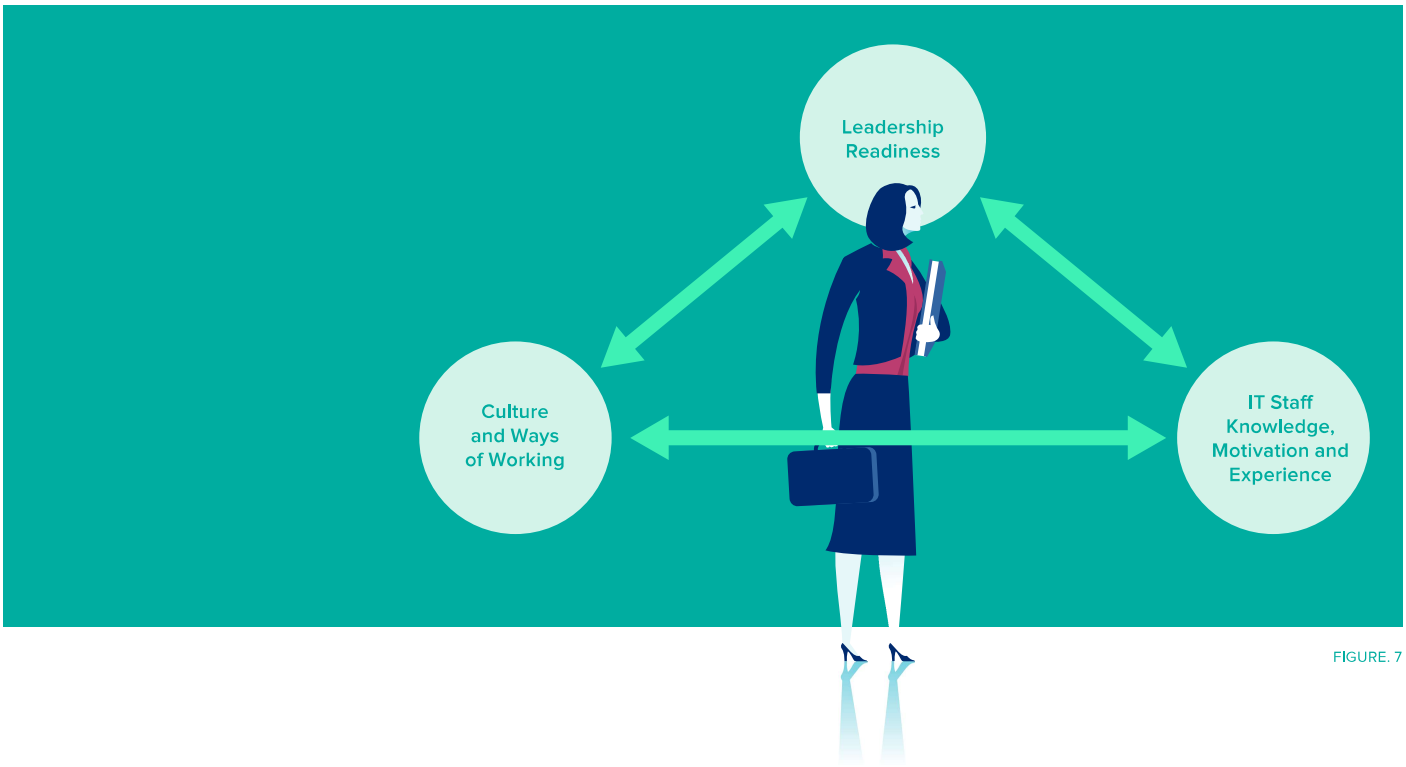


FIGURE. 7

Lack of Cloud Expertise or Cultural Readiness

Interestingly, in our survey a lack of cloud expertise or cultural readiness was rated as somewhat less important than regulatory concerns (see Figure 8 below). But it was still clearly important, and more of a concern for respondents who were more knowledgeable about the cloud. In other words, having more experience of migrating to the cloud results in a greater appreciation for the people challenges. We believe that this highlights the danger of focusing on the cloud as a technical problem and the tendency of people to only understand the importance of people to the success of cloud implementation after things go wrong.

Percentage of Respondents who Selected these Challenges as one of the top three Challenges Presented by the Cloud

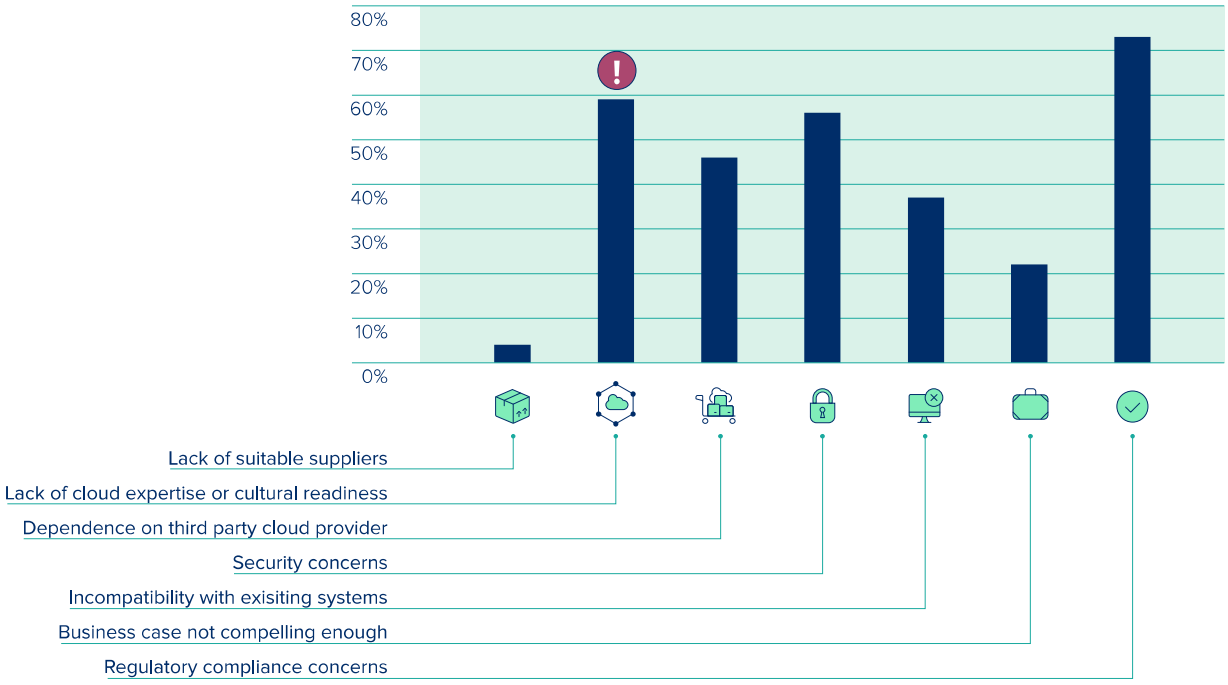


FIGURE. 8

Based on 191 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021). Respondents to the survey were asked to pick the three most important challenges of the cloud.

The People Challenge in the IT Department

One theme that came through clearly in our research was the difficult people challenges that arise in IT departments both before a move to the cloud and as the transition to the cloud proceeds. As depicted in Figure 9, these challenges appeared in three ways.

The People Challenge in the IT Department

FIGURE. 9

First, the move to the cloud requires new IT skills and competencies, therefore impacting the organisation from a talent perspective. While adopting cloud infrastructure and associated services may feel like outsourcing, in the sense that some talent challenges are moved to CSPs, it is always the case that new skills will be required to manage cloud infrastructure. Clear consideration needs to be given to how this talent will be acquired or developed.

Previously, IT departments would have had a deep knowledge of developing and maintaining applications running on an on-premise system. Now, they need to change focus to knowing how to manage relationships with CSPs, as well as expertise in cloud security and the development and management of applications that will run on the cloud. Even more importantly, they need to understand what the cloud can do in addition to a simple lift and shift of existing applications if cloud implementations are to succeed. This requires significant re-tooling of existing personnel, as well as hiring new staff with key skills at a time when very few of these individuals are available.

Second, there are some IT personnel whose skills will simply no longer be needed. Individuals with expertise of the intricacies of running the on-premise system were the foundation of success prior to the move to the cloud. Furthermore, these individuals are often long-term employees with broad social networks who are deeply embedded in the organisation. But the reality is they may simply not be needed to support the move to the cloud. Crafting a plan to redeploy these individuals is often a key part of moving cloud adoption forward. In fact, for some firms we interviewed, the challenges of dealing with this group was a significant barrier to the transition to the cloud.

Finally, the move to the cloud has significant implications for the budget of the IT department and the prestige and the influence of various teams within it. This can result in an IT department where enthusiasm for a move to the cloud is muted or, at worst, seen as a threat and actively blocked. When this occurs, careful management is needed to ensure that there is an alignment of interests, with the transition to the cloud seen as being to the benefit of everyone in the IT department.

Culture and Ways of Working

> "As digital transformation grows, the lines between IT and business are becoming increasingly blurred. Organisations look to the cloud paradigm as a means of achieving greater flexibility and adapting swiftly to regulatory change and evolving business needs. This is why DevOps and Agile are also beginning to play a leading role away from traditional IT areas."
>
> Marco Noli, Executive Partner, Reply (UK & France), May 2021

While DevOps defies simple definition, it is a compound of development and operations that seeks to improve collaboration between those teams. It is a culture change focusing on rapid IT service delivery through the adoption of agile and lean practices, in the context of a system-oriented approach. DevOps emphasises people (and culture), with implementations utilising technology — especially automation tools that can leverage an increasingly programmable and dynamic infrastructure from a life cycle perspective (see Figure 10 below).

The DevOps Loop

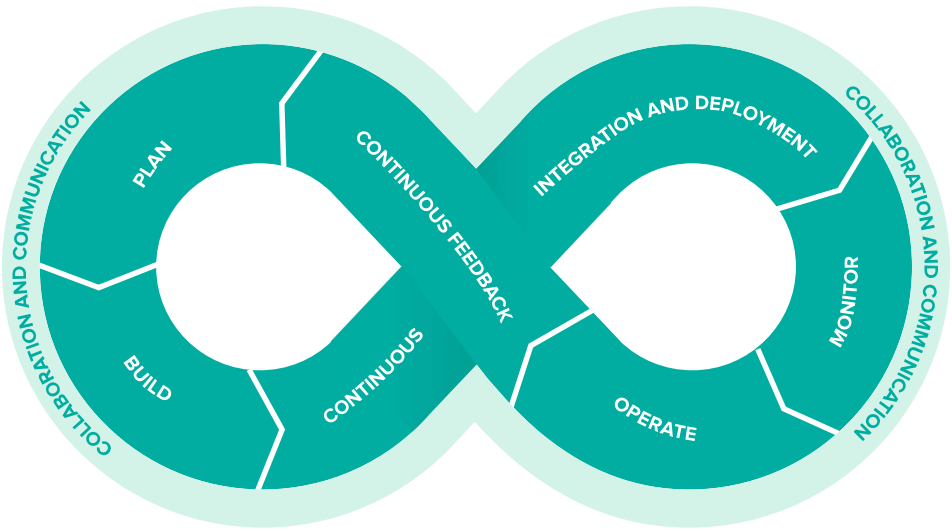


FIGURE. 10

(Adapted from Dustin Whittle, 2013)

The transition to DevOps requires fundamental change. First, it requires a culture where open communication and a tolerance for mistakes become core values. Second, the introduction of Continuous Integration and Continuous Delivery (CI/CD) means that the separation between development and operations is removed. The silos in which these different functions worked is replaced by ongoing collaboration and cross-functional teams in a fundamental reboot of working practices. Finally, new digital tools are introduced to manage the process of developing and operating new apps in an entirely new way.

Moving to DevOps as a part of the transition to cloud is crucial. In a recent study,[5] Atlassian, the Australian software company, found that organisations using DevOps ship higher quality deliverables (61%), with increased deployment frequency and faster time to market (49%). It is not just organisations who reap the benefits either; practitioners say they have learned new skills (78%) and received a raise (48%). The benefits of DevOps also explain why some financial institutions choose to transition their development activity to the cloud while still running the resulting applications on premises.

Leading the Transition to the Cloud

> "To be truly successful and actually add value (in particular, in terms of access to innovation and agility), transitioning to the cloud requires a new way of thinking; it requires cultural change. Importantly, that is not just an IT issue. This cultural change has to be company-wide; it is perhaps the most important factor in an organisation's cloud strategy."
>
> Roman Koch, CIO, Baufinex GmbH (part of Bausparkasse Schwäbich Hall), May 2021

The transition to the cloud also raises important questions about the cloud readiness of leaders in the IT departments, the C-suites and the boards of financial institutions. If a cloud implementation is successful, it has strategic ramifications that will permanently disrupt business as usual, reshape the business model, and create whole new areas of activities.

But is the leadership team ready? This question is often easier to answer when it comes to technology leadership. From our research, the leadership of the IT department generally understands the technological advantages of the cloud and is ready to lead the migration from the IT perspective. But this is only part of the story.

What is often missing is a deep understanding of the strategic implication of a migration to the cloud in the C-suite and among board members. The cloud is too often seen as a technology issue, of concern to the chief technology officer (CTO) but not particularly important to the rest of the leadership team. This is because the organisational and strategic implications of migration are often not well understood, if at all, beyond the CTO. As such, the migration to the cloud is framed as a business decision where a focus is on costs and potential savings, rather than a strategic move with radical implications for how the financial institution will provide new value to customers and employees.

This is deeply unfortunate and dangerous. Financial services is rapidly becoming a technology business. As we heard on several occasions, "we are no longer a bank, we are a technology company". But do the C-suite and the board have the necessary knowledge and understanding to run a technology company? If incumbent firms are to successfully fend off new digital first fintech ventures, they need to be able to rapidly adopt and apply new technologies, including the cloud. Hard questions need to be asked about the technology acumen of top management and boards if financial services firms are going to make this transition. But where, as one interviewee put it, do we find "the sheep with five legs"?

[5] 2020 DevOps Trends Survey, Atlassian and CITE Research, 2020, 38 pages.

In summary, the journey to the cloud is not simply a technology problem. For any transition to the cloud to produce the sorts of benefits that it has the potential to deliver, significant organisational change is required, and the right people with the right skills must be in place. This does not just mean in the IT department, but also that the C-suite and the board are ready to lead a company that has transitioned to the cloud. This also means that any roadmap for the transition to the cloud needs both an HR plan and a budget to deal with organisational change and getting the right people in the right places with the right skills and experience. It is only by dealing with people and organisational issues upfront that the journey to the cloud can really succeed.

Key Leadership Questions on People and Culture

Executives and board members should understand the people and culture changes that the financial institution must address when transitioning to the cloud.

Some key questions leadership should ask on the readiness of people and culture for the transition to the cloud include:

People:

- Does the organisation have the right skills in place in the IT department?
- Does the organisation have a plan for redeploying the IT experts who have been running the on-premise systems?
- Is the IT department supportive of a move to the cloud?

Culture and ways of working:

- Are the organisation's ways of working appropriate get the most out of the transition to the cloud?
- Does the organisation have the right culture to support DevOps?
- Does the organisation have the right tools in place to support DevOps after transition?

Leadership considerations:

- Is the C-suite ready for the transition to the cloud? Do they have the right knowledge and strategic appreciation of the potential and challenges of cloud?
- Does the board appreciate and understand the potential and challenges of the cloud?

Section 6

Cloud Security

Leading the Transition to the Cloud

> "A cloud security baseline does not replace the existing processes and procedures already in place but builds on them. Its purpose is to identify security related business risks and provide risk mitigation to define a way of working securely in cloud. Whilst this may mean a mind shift from the 'old' ways of working, it does mean a 'cloud' relevant approach is adopted and is a fundamental cornerstone of a successful transition to cloud."
>
> Andy James, Partner, Cluster Reply UK (Microsoft Azure Gold Partner), October 2020

Until recently, security was the sticking point for financial institutions contemplating cloud adoption. But today, many in the industry, emphasise that a transition to the cloud can actually improve digital security compared to traditional on-premise systems. That shift in perception may provide some explanation for a strange paradox unearthed by our survey. But, before we turn to the survey results, let us recap what is meant by cloud security.

Cloud Security and the 'Shared Responsibility Model'

Cloud security is one of the highest priorities for financial institutions when they contemplate using the cloud. The Cloud Security Alliance, an international organisation dedicated to defining and raising awareness of best practices to ensure a secure cloud computing environment, defines cloud security as *"everything a security team is responsible for today, just in the cloud. All the traditional security domains remain, but the nature of risks, roles and responsibilities, and implementation of controls change, often dramatically."*[6]

As noted in Section 1, *Cloud Adoption in Financial Services: Where are we today?*, cloud computing involves a shared technology model in which the financial institution and the CSPs are implementing and managing different parts of the technology stack. Figure 11 illustrates the varying degree of security responsibility as a function of the cloud service model choices made by the financial institution.

[6] Security Guidance, Cloud Service Alliance, 2021, page 20.

Cloud Security as a Function of Cloud Service Models

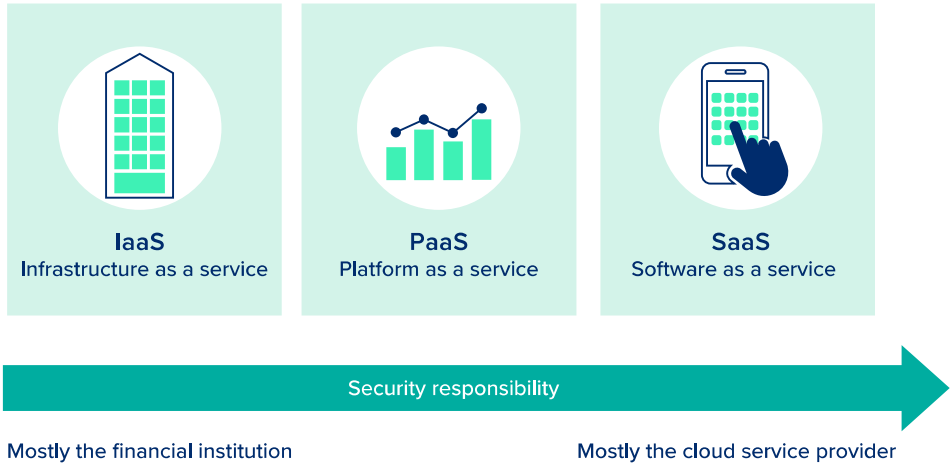


FIGURE. 11

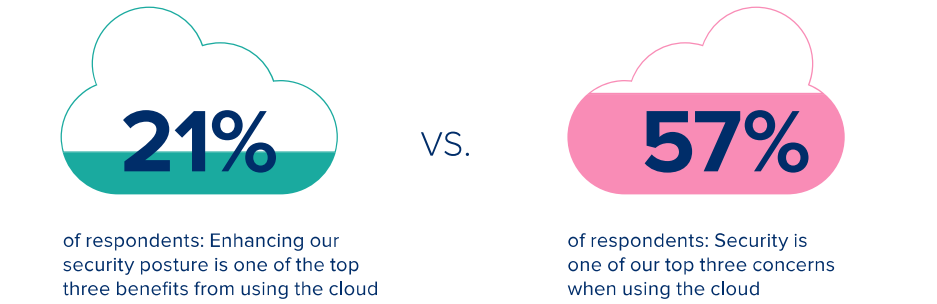
(Adapted from the Cloud Security Alliance)

- **SaaS:** In this model, the CSP commits to managing the majority of the security structure, as users within the financial institution are only permitted to access their specific applications, without the possibility to change these applications;
- **PaaS:** This is a more evenly distributed share of responsibilities model where the CSP is in charge of the security of the platform, while the financial institution is responsible for all changes and new developments of its applications, including the specifics of security configuration; and
- **IaaS:** As with the PaaS, the CSP manages the core security, while the financial institution is responsible for all developments on the cloud infrastructure. From a security perspective, this model therefore places a higher degree of responsibility on the financial institution compared to the PaaS model.

The Cloud Security Paradox

As alluded to in the introduction of this section, security is perhaps the matter for which our survey unearthed the most striking paradox. A large percentage of respondents noted that the cloud significantly enhanced their security position vis-à-vis traditionally hosted systems, while at the same time many respondents stressed that security concerns were among the most challenging issues encountered in transitioning to the cloud. Figure 12 provides an overview of this paradox.

The Cloud Security Paradox



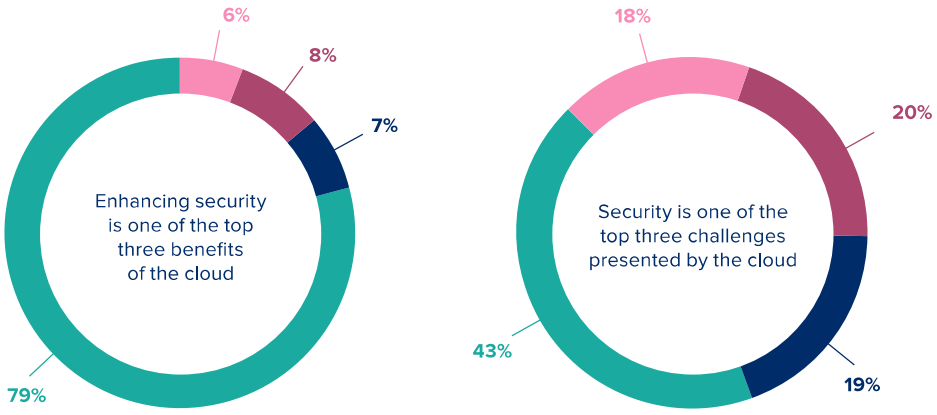


FIGURE. 12

Based on 191 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021). Respondents to the survey were asked to pick the three most important challenges and benefits of the cloud.

The divide among the industry practitioners who responded to our survey was also present among the senior industry leaders we interviewed. Interestingly, there were three factors influencing their stance on cyber security and cloud:

First: The cloud maturity level reached by their financial institution. Financial institutions appeared to reconsider their initial stance on cybersecurity, and become more comfortable with the cloud from a security perspective, as their cloud journey progressed and they implemented techniques, methodologies and tools to enhance their cloud security.

Second: We noted a significant difference between the retail world and the institutional world, particularly with respect to data privacy considerations. In the institutional word, for example, senior leaders in securities services stressed that cybersecurity was at the core of their cloud adoption projects. However, many of those senior leaders underlined that – despite the firepower of the CSPs – much remained to be done before they could consider moving critical applications to the public cloud, in particular due to data privacy concerns.

Third: Deployment and service models (refer to Section 2 for an overview of these models) significantly impacted their position regarding cloud security (and the related assurance requirements they sought from CSPs):

- With deployment models, for example, several leaders noted that their organisations felt more comfortable with private cloud services than the public cloud because of the perceived ability to tailor the architecture to meet their specific security needs. Others noted that, while they had originally started with private cloud services only, their organisations had gradually embraced public cloud services and implemented technical controls to ensure that their data was adequately protected.
- With service models, SaaS offerings were perceived to present a higher level of risk than both IaaS and PaaS, unless well architected.

The Enablers of a Strong Cloud Security Posture

The interviews with these senior leaders and the projects conducted by Reply in financial services, as well as other industries that the financial services industry can learn from (e.g., defence, healthcare, telco), resulted in a range of findings that would fill a whole report on the topic. In this section, we elected to highlight three specific areas:

- The need to distinguish between the 'security of' and the 'security in' the cloud;
- The need to adapt an organisation's existing security framework to the cloud; and
- The concept of security by design.

'Security of' and 'Security in' the Cloud

As noted above, security is a shared responsibility between the financial institution and the CSP. In general, the financial institution is responsible for the security of things running in the cloud while the CSP is responsible for the security of the cloud itself. For example, in AWS's Shared Responsibility Model, depicted in Figure 13:

- the CSP (AWS) operates (and is responsible for) the components from the host operating system down to the physical security of the facilities in which the service operates; and
- the financial institution assumes responsibility for the guest operating system (including updates and security patches), other associated application software as well as the

Illustrative Shared Responsibility Model

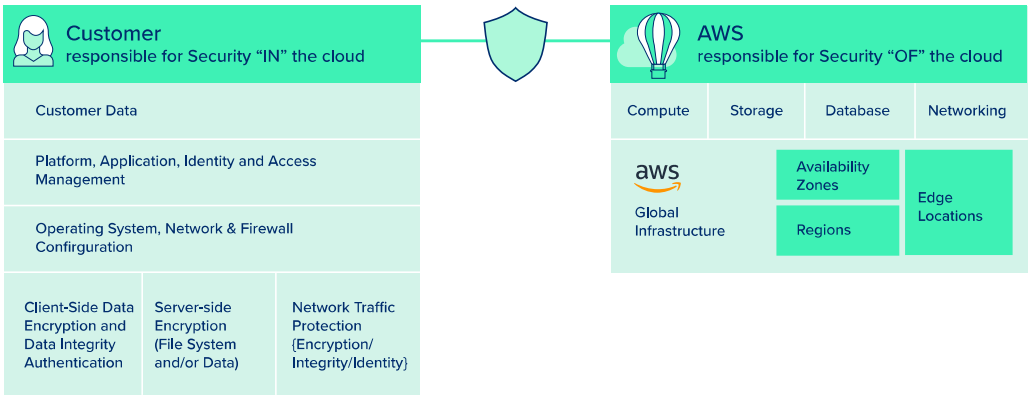


FIGURE. 13

(Adapted from AWS)

configuration of the security group firewall provided by the CSP.

Based on this shared responsibility model, the senior leaders we interviewed stressed two important elements to consider which echo Reply's own experiences:

- The need for clear accountability: A well-understood and agreed-upon shared responsibility model (or matrix) is a pre-requisite for ensuring that appropriate security controls are enforced. A clear understanding of what the CSP is responsible for and how they are applying controls must then be cross-referenced with the requirements of the organisation.

  The CSPs assert that financial institutions can strengthen their security posture, using multi-layered, built-in security controls and unique threat intelligence from CSPs to help identify and protect against rapidly evolving threats. While the interviews and Reply's experience suggest that this is often true, the fact that a financial institution is relying on a CSP does not change the fundamentals of understanding the security posture, the appetite for risk, and applying the appropriate control framework.

  It does mean clarity is required on accountability for specific controls. As one of the global CTOs we interviewed put it: *"This clarity should be achieved through clear application of the organisation's security framework and understanding the accountability of the CSP and the organisation for specific controls".*

> "We mustn't forget that the accountability for everything still remains with the executives and the Directors of the financial institution. Even though you are using a service provider, you have to think of it as an outsourcing contract. You retain the accountability if anything goes wrong. You need to have good risk management of that service provision."
>
> Jeremy Arnold, Chief Risk Officer, Natwest Markets, May 2020

- Changing the line of questioning: Without taking security of the cloud for granted, a financial institution may therefore want to change its line of questioning from 'is the cloud secure?' to 'how do I operate securely in the cloud?'

  Many of the senior leaders we interviewed noted that this is not an easy conversation to have, whether with the board and the C-suite or the regulatory community.

Adapting the Security Control Framework to the Cloud

The senior leaders we interviewed pointed to a common flaw in cloud security: too often a financial institution's cloud security posture is assessed starting from a control framework that has been designed for the on-premise world. It therefore assumes that the institution has control over the underlying infrastructure.

> "Institutions that fail to review and update their cyber security control framework when transitioning to the cloud should expect a long list of controls that are not applicable and, of more concern, security gaps.
>
> Luca Mayer, Senior Manager, Spike Reply Italy, April 2021

Adopting the cloud requires that the security control framework be revisited, distinguishing between CSP and financial institution responsibilities, and supporting cloud native technologies along with their distinctive paradigms.

Security by Design

"In a relatively short time, we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters."[7] So tweeted Jeff Jarmoc, head of security for Salesforce, in the aftermath of the distributed denial-of-service attacks on October 21, 2016. It epitomised a key issue raised in the discussions we had with senior leaders: security does not work if it is an afterthought – it needs to be built in by design. This is true in all industries, and financial services is no exception.

The issue is compounded by two elements present across the industry:

- First, as traditional financial institutions are transitioning to the cloud, they have to rethink their overall IT security posture. This often leads to a complex hybrid environment that combines legacy on-premise with cloud-based infrastructure, applications, and services; hardly security by design. This remains a challenge for CSPs and financial institutions alike, and the focus of much attention by boards, the C-suite and regulators.
- Second, the increasing pace of innovation powered by DevOps (refer to Section 5) can undermine the important discipline of securing infrastructure, applications, and services – an integral part of ensuring security by design.

As a result, some of the financial institutions we talked to are now embracing DevSecOps, essentially turning developers into security engineers. The aim is to balance the need for development speed and agility with the requirement to minimise the risk of security failure.

[7] Jeff Jarmoc on Twitter, October 22, 2016.

> "DevSecOps injects security into the DevOps process, providing a structural assurance that code will be designed with security in mind. This is a game changer to operate mission-critical workloads in the cloud."
>
> Cloud Enablement Program Manager, Global Systematically Important Bank, May 2021

In summary, as financial institutions are increasingly turning to the cloud, they have recognised the need to adapt their traditional methods of cyber security protection to the world of the cloud. Our survey suggests that the actual and perceived maturity of the industry in this area lags behind other aspects of cloud adoption; it is nonetheless a pre-requisite that the industry needs to address successfully to meet the pressing needs of business without compromising security.

Key Leadership Questions on Cloud Security

Executives and board members should understand the cloud security challenges that the financial institution must tackle when transitioning to the cloud.

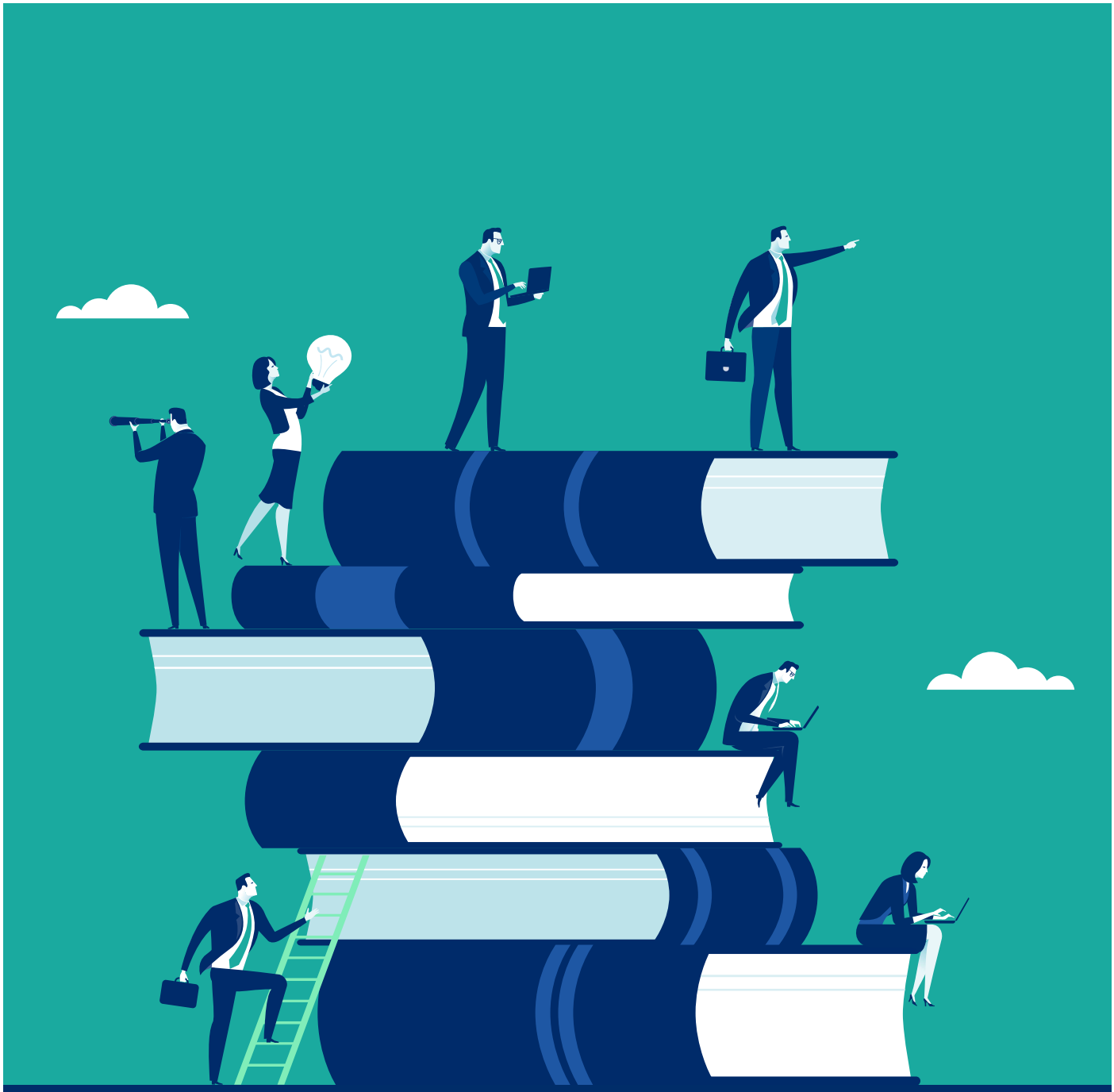
Some of the questions that a financial institution may consider regarding cloud security include:

Accountability:

- Is there clear accountability for delivering security controls according to the organisation's risk control framework?
- How is this recorded, agreed, approved and regularly reviewed and updated?

Cloud security risk assessment:

- What cloud specific additional vulnerability scanning and other risk assessments will be implemented by the Chief Information Security Officer (CISO)?
- How will remediation of any control gaps be managed?
- What (audit) process is required to ensure cloud specific risk is within risk tolerance?
- What are the plans to report cloud specific security updates to the Audit or Risk Committee(s) and how will subsequent actions be followed?



Section 7

Cloud Regulation

> "The cloud is a facilitator. It brings flexibility, it enables innovation. The challenge with the cloud is that you are putting a lot of dependencies on a very small number of key external providers. Regulators are worried about the systemic risk dimension of cloud service providers and the ability to enforce and prioritise recovery if one or more of them were to fail. Using the cloud is relying on outsourcing that is critical to day-to-day operations; the key question is 'what happens on a bad rainy day."
>
> Frédéric Mouchel, Chairman of the board of Directors, Royal Bank of Canada Investor & Treasury Services, April 2021

Cloud computing is not governed by a direct regulation or a specific cloud related law. The legal and regulatory landscape is made up of a matrix of different rules and regulations, spanning multiple industries and geographies.

The stance of regulators varies greatly across geographies and is continuously evolving. As recently as August 2021, the Handelsblatt – Germany's leading business newspaper – published an article on how the Bundesbank, Germany's central bank, is now encouraging German banks to use more cloud applications. *"The cloud strengthens the innovative strength of banks and also gives smaller banks access to technologies that only large banks with extremely powerful data centres could afford,"*[8] emphasised Prof. Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank in charge of Banking Supervision, Information Technology and Risk Control.

In shedding light on the steps taken by regulators to lower existing regulatory hurdles for cloud adoption by financial institutions, Prof. Wuermeling also stressed that financial institutions embracing the cloud had to carefully consider applicable outsourcing regulatory requirements (e.g., *"an exit strategy must always be considered."*[9])

In summary, our research and survey have highlighted that the cloud – from a technology standpoint – is not (yet) in its end state; that too is true for the regulatory framework; it continues to evolve and is not harmonised. That probably explains in part the frustration expressed by the respondents of our survey when implementing cloud solutions and dealing with regulatory requirements.

[8] *"Die Cloud stärkt die Innovationskraft der Banken und verschafft auch kleineren Banken Zugang zu Technologien, die sich nur Großbanken mit enorm leistungsfähigen Rechenzentren leisten könnten"*, Prof. Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank, quoted by the Handelsblatt on 8 August 2021.

[9] *"Eine Exit-Strategie muss immer mitgedacht werden"*, Prof. Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank, quoted by the Handelsblatt on 8 August 2021.

Regulatory and Compliance Concerns: The Number One Challenge!

As noted in Section 1, *Cloud Adoption in Financial Services: Where are we today?*, respondents of our survey singled out regulatory and compliance concerns as the Number One challenge of using the cloud.

What are the Challenges of Migrating Systems to the Cloud?

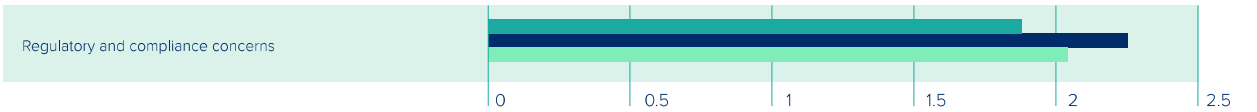


FIGURE. 14

Based on 191 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021). Respondents to the survey were asked to pick the three most important challenges of the cloud. In the analysis, a value of "3" was given to the first item picked, "2" to the second item and "1" to the third item selected.

Our interviews with senior leaders in the industry would suggest that the concern is particularly acute in certain regions (e.g., the Middle East) and countries (e.g., several senior leaders indicated that a few specific countries in Europe have adopted a more stringent stance than others), consequently making it more difficult for global financial institutions to take full advantage across jurisdictions of the capabilities enabled by the cloud.

Beyond the differences they encounter across countries, the senior leaders we interviewed also raised concerns about the lack of harmonisation amongst regulatory and supervisory authorities responsible for specific segments of the financial sector. For example, within the European Union, some noted counter-intuitive divergences between the European Banking Authority (EBA) Guidelines on outsourcing arrangements – which include a set of requirements for outsourcing by banks, including cloud computing services – and the Guidelines issued by the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Market Authority (ESMA).

There is a lot of work in progress at the international and regional level to address some of these concerns. In the European Union, for example, the European Commission's draft Digital Operational Resilience Act (DORA) includes wide-ranging proposals to regulate digital operational resilience in financial services in a more harmonised way. But the DORA introduces yet another issue that will no doubt shape the use of cloud going forward, i.e. regulatory requirements pertaining to operational resilience.

Operational Resilience

As noted in the quote by Frédéric Mouchel at the beginning of this Section, *"the key question is 'what happens on a bad rainy day'..."*

This issue – from a systemic risk perspective – was also stressed by the Financial Stability Board (FSB) in its November 2020 Discussion Paper: *"Potential systemic risk could arise if, for instance, a sufficiently large number of financial institutions (or a single systemic financial institution) became dependent on one or a small number of outsourced or third-party service providers for the provision of critical services that were impossible or very difficult to substitute effectively and in an appropriate timeframe. Where there is no appropriate mitigant in place, a major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple financial institutions."* [10]

On the international scene, the Basel Committee on Banking Supervision enacted in March 2021 Principles for Operational Resilience *"to strengthen banks' ability to absorb operational risk-related events, such as [...], cyber incidents, technology failures [...], which could cause significant operational failures or wide-scale disruptions in financial markets."* [11]

Within the European Economic Area (EEA), DORA will (when adopted) not only introduce a harmonised set of rules and requirements for the provision of cloud computing services, covering similar areas as the current Guidelines issued by the EBA, EIOPIA and ESMA, it will also introduce a harmonised approach to the supervision of the cloud service providers, including an EEA-wide collection of data on these cloud service providers to better understand the risks and dependencies from a systemic perspective too.

In summary, regulatory compliance remains a significant challenge for institutions embracing the cloud. While regulators are working with the industry and cloud service providers to address this issue, two key themes that will no doubt influence the future of cloud regulation are 'concentration' (both in terms of 'concentration of supply' and the 'sheer number of capabilities that are integral to the running of financial institutions and market infrastructure that are moving to the cloud') and 'transparency'. Beyond existing and future regulatory requirements, financial institutions must understand the risk and resilience of the cloud solutions they adopt.

[10] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, Discussion Paper, Financial Stability Board, 9 November 2020, page 2.

[11] Principles for Operational Resilience, Basel Committee on Banking Supervision, March 2021, page 1.

Key Leadership Questions on Regulation and Compliance

Executives and board members should understand the regulatory implications of adopting the cloud.

Some of the questions that a financial institution may consider from a regulatory standpoint include:

- What are the regulatory and compliance implications of the proposed cloud solution?
- Can the proposed cloud solution deliver the performance, availability and resilience in line with current regulatory requirements and supervisory expectations? What is the likely impact of 'looming' regulatory changes on this assessment?
- Does the proposed cloud solution require ex ante approval by one or more supervisory authority, ex ante notification or ex post notification (e.g., under applicable outsourcing regulatory requirements)? What are the primary challenges to be expected at approval/ notification stage and, then, on anongoing basis (e.g., from an oversight perspective)?
- Does the cloud service provider provide audit rights for the institution and all relevant supervisory authorities?
- What are applicable data residency requirements and how will the organisation evidence compliance with these requirements?

Section 8

Data Management, Governance and Integration

> "There is an obvious trade-off between the benefits and the risks of the cloud when it comes to 'data assets' and, to an extent, fundamental differences in terms of appetite between business lines. Within asset management, for example, there is a strong appetite to leverage cloud capabilities in terms of data science and data analytics to drive incremental business value. Within wealth management, by contrast, there can be more reticence: As a private banker, you are in effect the guardian of your clients' data."
>
> Peter Wintsch, Chief Technology Officer, Pictet, June 2020

It is increasingly common for senior executives and commentators to express the growing importance of data to the business models of many financial services firms in one-liners such as *"we are sitting on a data gold mine."* While this is true, the other side of the "data coin" – and one that most firms increasingly recognise – are the risks associated with holding and processing large amounts data (e.g., from a breach or leak) and the challenges of maximising the value derived from the data while ensuring compliance with the myriad of existing regulations.

These benefits, risks and challenges are made all the more complex with the adoption of the (public) cloud. Moving data out of the financial institution creates a series of challenges, including securing sensitive data such as personally identifiable information or intellectual property, complying with data privacy regulation and understanding what 'data assets' are effectively available and how they might be combined.

In this section, we cover three areas that were specifically highlighted by the respondents of our survey and the senior industry leaders interviewed. These came about during discussions of how financial institutions can best reap the benefits of the "data goldmine" by leveraging the cloud.

The Cloud and the Dynamics of Data Management

When a financial institution wants to leverage data assets and/or become a more data-driven organisation, it will typically generate and use much more data. This data can include both structured and unstructured data and be both internal and external to the firm. This can quickly overwhelm on-premise resources for storing and processing data. Our interviews with senior leaders in the industry would suggest that moving to the cloud is generally perceived as the most effective solution.

Typically, the institutions they represent leverage the cloud because of elasticity of compute and storage capacity, flexibility to bring compute and data together, and agility and pace. In their view, this transforms the dynamics of data management in fundamental ways and calls for the transformation of data operations in a way that their organisation focuses its energy on actually using data to create value rather than manipulating them. This view was largely echoed by Bipul Kumar, Practice Lead - Data Analytics, Google Cloud UK&I, as he was sharing his experience at Episode 7 of Reply's Webinar Series on Cloud in Financial Services (see Figure 15).[12]

[12] The Series is available at https://www.reply.com/en/topics/cloud-computing/cloud-in-financial-services.

Simplified Data Operations

Quick	Scales	Easy Accessibility	Automatic high-availability	Automatic snapshots and data backup
				
Set up service in seconds and query immediately	On-demand per your business needs from terabytes to hundreds of petabytes	Transparent, free data compute replication in multiple locations makes your data available for query even in the case of extreme failure modes	With no extra charge and no additional setup	Reduces worries and unexpected data changes

FIGURE. 15

(Presented by Bipul Kumar, Practice Lead - Data Analytics, Google Cloud UK&I, at Reply's Webinar on Cloud in Financial Services on 8 September 2020)

In keeping with our own experience, the senior industry leaders we interviewed stressed that this step has been the prerequisite to bring in artificial intelligence capabilities without requiring an inordinate amount of time to replicate or move data. Transforming data operations is widely regarded a prerequisite to unlock the value of data and fast-track machine learning capabilities.

Data Governance

The second theme that repeatedly came up is data governance. Respondents to our survey noted that data governance in the cloud was among the issues most in need of improvement. Respondents were requested to rate how well various aspects of cloud governance were developed on a scale from 1 (not developed at all) to 5 (very well developed). As depicted in Figure 16, 59% of respondents noted that data governance requires (significant) improvement or was not developed at all.

Data Governance Maturity Assessment

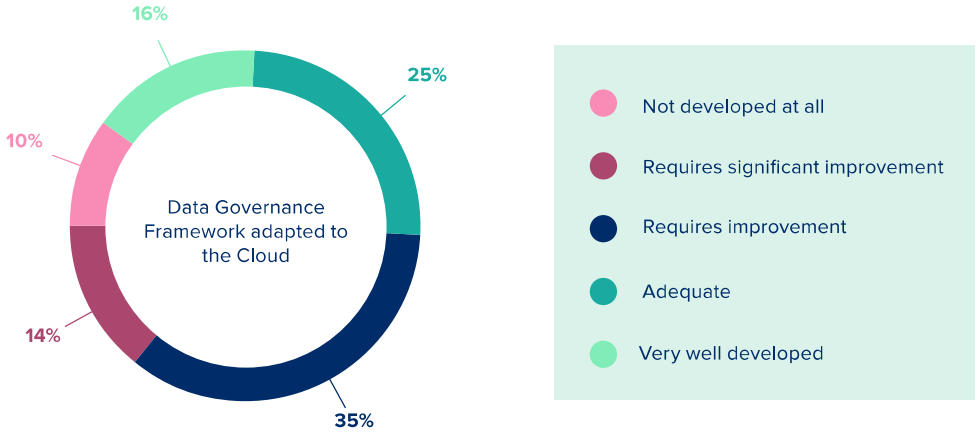


FIGURE. 16

Based on 177 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021). Respondents to the survey were asked to rate how well these various aspects of cloud governance were developed in a scale from 1 to 5.

The ultimate goal of data governance is to ensure that the data is reliable and consistent so that it enables the financial institution to undertake key business activities and gain further business insights, while ensuring that the data is being used in a compliant and ethical fashion. The responses to the survey suggest that the financial services industry needs to handle data governance differently as cloud adoption continues.

Indeed, when looking back on where the industry has come from, financial institutions used to have their own data centres, their own 'tin and wire'. That is no longer the case for many firms who have, instead, transitioned (partly) to the cloud. Data volumes have increased exponentially and the diversity of data types and sources – both structured and unstructured – has increased. In short, the way data is handled has changed and there is a much lower tolerance for low data quality. This is obviously compounded by additional factors, including regulatory requirements as well as opportunities provided by technology and data science.

As a senior industry leader put it in one of our interviews, *"financial institutions must address these changes introduced by the cloud when facing into data governance. They need to consider a 'cloud first data governance framework.'"*

In our experience, this will typically entail the traditional considerations about security, privacy and compliance but also the question as to how we handle data in ways that it is more visible to user groups, how it can be more accessible, and more instant whilst maintaining robust controls and risk management processes.

Data Integration

While the survey did not expose particular issues with data integration, the interviews we conducted corroborated our experience derived from cloud projects in financial services as well as in other industries: As financial institutions migrate data and applications to the cloud, they face the significant complexities that come with integrating disparate data sources.

A typical scenario may be a firm with hybrid environments, including mission critical applications that are now fully cloud-based, applications that still run on premises, data sitting across multiple cloud service providers, and hybrid workloads with data sitting, and being processed, both in the cloud and on premises.

In these scenarios, the financial institution faces multiple technology and organisational challenges. In the words of a senior industry leader: *"First, we faced a high volume of disconnected and distributed data sources and data types that we needed to try to bring together. Second, we needed to do mass integration at scale. And, third, we had to deal with legacy data transformation processes that we had implemented over time, including poorly documented ETLs."*

Our experience and the interviews we conducted suggest that successful firms elaborate and deploy thorough strategies to drive integration within the cloud, between different clouds, and between multiple clouds and the institution (hybrid workloads).

It is not only about moving applications and data to the cloud, but also about understanding the processes that underpin dataflows. The more firms understand them, the more they can embrace cloud-based automation.

In summary, there is a lot of talk about digging into the data goldmine, and leveraging the cloud. Whether the building blocks of the cloud can enable this or not is influenced by how financial institutions tackle the changes to data management and data governance that are required to avoid wasting that goldmine. From an architecture and engineering perspective, it does not stop there though. The third challenge – and hardly the least – is to deploy a robust data integration strategy to allow users to leverage the capabilities enabled by the cloud (e.g., analytics, machine learning) across traditional data silos.

Key Leadership Questions on Data Management, Governance and Integration

Executives and board members should understand the data governance implications of adopting the cloud.

Some of the questions that a financial institution may consider include:

- What are the institution's strategic objectives with respect to data and in what way does the cloud enable these objectives?
- How will the cloud transform the dynamics of data management within the institution? How is the institution proposing to deal with these changes?
- In what ways will the cloud affect the institution's data governance framework? How is the institution proposing to deal with these changes?
- What is the institution's strategy to drive data integration within the cloud, between different clouds, and between multiple clouds and the institution (hybrid workloads)?

Section 9

Journey to the Cloud

> "The timeline to migrate to the cloud and reap actual benefits from a cloud migration is a function of how well the migration is planned. A lot of organisations have had big cloud initiatives that have delivered very little. Underpinning a successful migration, there must be a maturity journey and strong governance processes that enable success rather than lead to inertia."
>
> Tim Falla, Partner, Glue Reply UK, October 2020

In this section, we will summarise some of the insights we have gained into the different ways financial institutions approach the journey to the cloud. It is clear from our survey that firms are at very different places in their migration to the cloud. Responses to the question "what is your organisation's cloud adoption maturity level" ranged from a small number of firms that hadn't even considered the cloud (<5%) to more than 10% whose applications run primarily on the cloud. We summarise the responses in Figure 17.

What is your Organisation's Cloud Adoption Maturity Level?

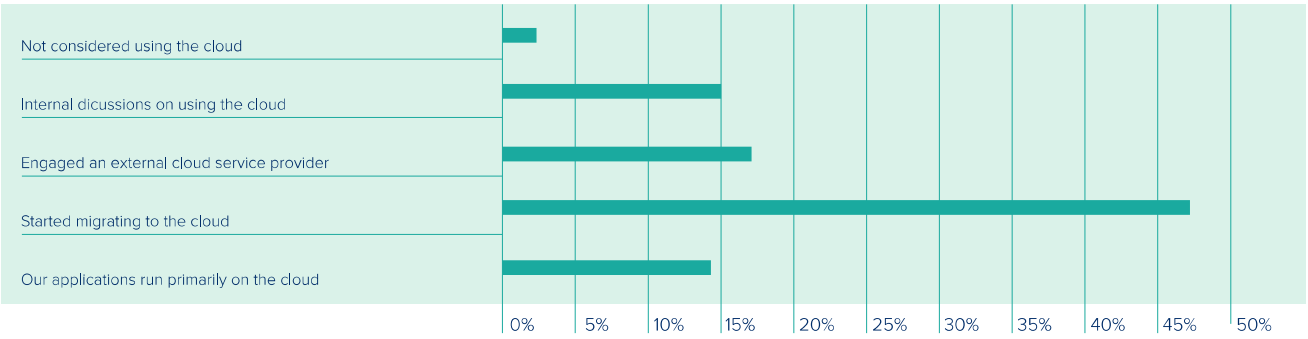


FIGURE. 17

Based on 177 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021).

Examining Figure 17, one notable result is that the majority of our respondents have started the journey to the cloud. Well over 50% are at least partially on the cloud or primarily on the cloud. Cloud is now the norm in financial services, and it will be increasingly difficult for any firm to provide a competitive offering without embarking on the journey to the cloud. It no longer is a question whether moving to the cloud is a good idea. Migrating to the cloud is now a proven route to efficiency and innovativeness and, in fact, is a necessary strategic investment to maintain competitiveness.

The Challenge of Technology Adoption

At the same time, the adoption of new technology is always a challenge. This is partially a reflection of the organisational change that is required to effectively engage with the technology. But it is also due to the fact that technologies change rapidly as they are widely adopted. Choosing a new technology is often to embark on a road with no clear endpoint, as the technology develops and new applications are invented by the growing community of users. The business case that justified the initial engagement often disappears and is replaced by far more profound changes as new opportunities are created by innovation inside and outside the firm.

For example, the early use cases for the PC involved simply moving current activities – such as the typing pool – onto networked PCs to allow the digital storage and retrieval of documents. But once organisations adopted PCs, the potential applications for the technology skyrocketed as internal and external innovators figured out completely new things to do with the new technology. No one anticipated the spreadsheet or e-mail when they ordered their first PCs, but these and other apps quickly became the dominant applications, creating much more change than was first envisaged.

What is Full Cloud?

This same process is happening with cloud. This raises an important question: what is full cloud? If the CSPs continue to innovate new services and firms engage more deeply with the cloud internally, then full cloud is somewhat of a moving target. For our purposes here we will consider full cloud adoption to have occurred when the majority of a firm's core development and operations takes place on the cloud. There will, of course, be some activities that are simply not worth moving to the cloud. For example, they may be phased out within a few years or are of such a small scale that transitioning to the cloud is not worthwhile.

But full cloud is not just about technology. Full cloud also has a cultural aspect. There may be good reasons (regulatory, client preference, cost) for having things on premises, but if the default expectation is that things will be on the cloud then that is a good indicator that a firm is full cloud. They are ready to compete with the cloud native firms that are increasingly threatening to attract customers away with new and transformational offerings.

Different Journeys to the Cloud

There are many ways to migrate activity to the cloud. In fact, no two journeys to the cloud are the same. But there are some common patterns that can be discerned. From our research four general approaches are common:

1. **Partial:** For some firms, the migration to the cloud is necessarily and purposefully partial. This might be due to regulations in their geographic context that prevent moving things to the cloud, or it may be because employees or customers are not ready. However, what distinguishes this pattern is an explicit plan to only migrate a certain activity or set of activities to the cloud without any plan for full migration at a future point. One common form of this approach is to use the cloud for the development of new applications that will then be run on premises. This allows firms to access the speed and innovativeness of the cloud in a development sandbox while leaving their systems running on premises and their data local.

2. **Incremental:** An incremental approach is one where the objective is to move all or most activity to the cloud, but to do it over an extended period and in manageable steps. For large firms, even this approach is quite challenging but may be necessary to reduce risk and disruption. It also provides more time to deal with the people and culture issues mentioned earlier. However, it also means the benefits and improvements in the customer and employee experience are incremental. So, while in some ways this appears lower risk and to require less resources, it is also expensive in others and potentially undermines the competitive advantage of the firm in ways that are hard to repair.

3. **Big Bang:** This is the most ambitious approach to moving to the cloud. As such it is most applicable to small and medium sized firms due to the complexity of moving the operations of a large financial institution to the cloud. In this scenario, the core systems of the firm are moved to the cloud in a single project over a relatively short period of time. The risk and upfront resources required are greater, but the impact is also immediate. The transformation of the organisation produces efficiency, scalability and innovation across the organisation in a short time frame.

4. **Cloud Native:** For some firms, of course, no transition journey is necessary as they are born on the cloud. We include being cloud native as it is useful for firms that are transitioning to the cloud to be aware that they are facing competition from firms who never had on-premise infrastructure or systems. These firms are rapidly scalable, highly innovative, and offer customer experiences that are hard to match with traditional approaches. For traditional financial institutions, thinking about established competitors as the benchmark is to miss that the real revolution is in firms that are cloud native. We find that thinking about the challenge of this reality often helps institutions as they figure out their cloud strategy.

> "At illimity, we had the chance to start from a greenfield situation. Being cloud native enables us to achieve faster time to market, to keep IT architectures simple and to be fully focused on the organisation's core business and strategy. Importantly, cloud infrastructures and services have achieved the right maturity to ensure regulatory compliance and a strong cybersecurity posture."
>
> Filipe Teixeira, Chief Information Officer, illimity bank, May 2021

These different journeys are often combined. Firms start out with a plan for partial cloud implementation and then move to incremental, only to find the pressures to accelerate adoption impossible to resist. They then jump ahead into a big bang implementation to rapidly take advantage of the scalability and innovation that comes with cloud implementation at scale.

In summary, while every firm takes a different journey, there are some clear patterns. While barriers may exist that make full adoption of the cloud unrealistic, the pace of adoption is quickening and most financial institutions have at least put their toes in the water. At the same time, traditional financial institutions face digital native entrants that were born on the cloud and are reaping the full benefits of the technology. Even in the medium term, it is clear that all financial institutions will need to move significant activity to the cloud in order to speed innovation, increase flexibility, and provide higher levels of customer service. It is no longer a question of when, but rather how firms transition to the cloud. The question of what journey each firm should take must be treated as a central strategic decision.

Key Leadership Questions on the Journey to the Cloud

Executives and board members should include discussions of their institution's journey to the cloud in the strategic plan of the organisation. The journey to the cloud is not just a technical question that can be left to the CTO alone, but a key strategic concern for the top management team. Some of the questions that a financial institution may consider regarding its journey to the cloud include:

Where is the organisation?

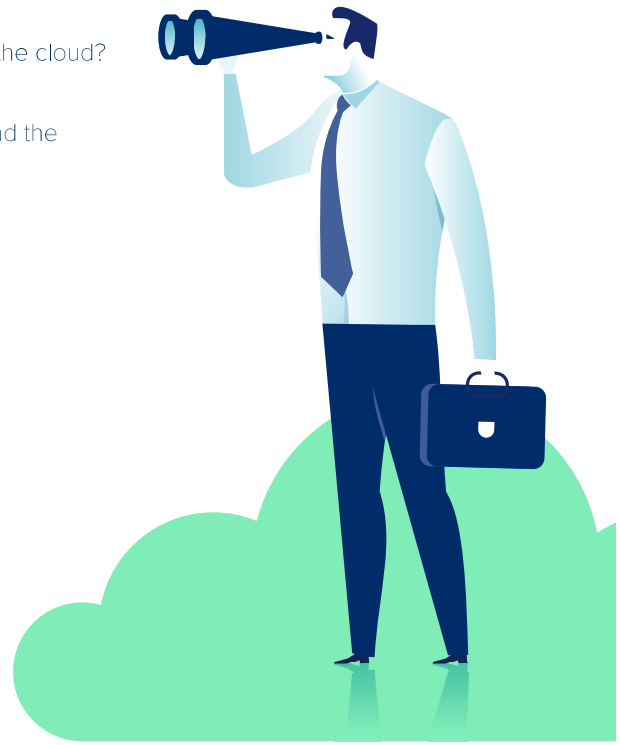
- Has the organisation started its move to the cloud? If not, why? What does the organisation need to do to get things moving?
- If the organisation has started its move to the cloud, which path is it on? How far has the organisation gotten and what are the barriers that are preventing the organisation from moving faster?

Where does the organisation need to be?

- Given the organisation's strategic goals, where does the organisation need to be in three years? In two years? What needs to happen right now to get the organisation moving in the direction the it needs to go?
- What strategic limitations is the organisation facing due to the current pace of cloud adoption? What opportunities could the organisation open up by increasing the pace of cloud adoption?

How is the organisation going to get there?

- What is the organisation's plan for moving ahead with its transition to the cloud? How will the organisation move ahead fast enough to match its competitors?
- What internal barriers may get in the way of the organisation's transition to the cloud? How will the organisation overcome these barriers?
- What does the organisation need to learn about the cloud to be able to lead the transition to the cloud?



Section 10

Leveraging the Cloud to Fuel Innovation

> "The adoption of cloud agnostic software development has been part of MeDirect's strategy to become a technology leader in the financial sector. Developing applications to be able to run on cloud-agnostic platforms allows MeDirect to hyper-scale and to take advantage of all the benefits of cloud providers, allowing for the future growth of MeDirect without any potential limitations."
>
> Chris Portelli, Chief Technology Officer, MeDirect, May 2021

While efficiency and scalability often dominate discussions of the reasons for cloud adoption, respondents to our survey rated "enables innovation" as the second most important benefit of moving activity to the cloud. Perhaps equally important, the more knowledge and experience a respondent had the more highly they rated innovation as a benefit.

Approaches to Innovation on the Cloud

From our research, we identified four different ways that firms engaged in innovation on the cloud. First, 17% of respondents said that they used the cloud to speed up the development and testing of software that would then be run on premises. Historically, developers have had to wait for machines to be available to code, test and debug systems. With the cloud, sandboxes can be setup for that work, dramatically speeding up the development process. Furthermore, these sandboxes can be shut down when not required. As a result, even in cases where moving operations to the cloud was not feasible or desired, we saw many firms that recognised moving development to the cloud increased the speed and effectiveness of software development.

Second, and perhaps somewhat surprisingly, 30% of respondents are developing and running software on the cloud while ensuring that the applications can be run on premises if necessary. From our interviews, this reflects one of two perspectives (or a combination of both). On the one hand, it may reflect a concern that applications may need to be moved back on premises if problems are encountered with cloud-based operations. Second, this was often a way to ensure that applications could be moved from one CSP to another. By not using any of the cloud specific features, this ensured that nothing that was unique to a particular provider was built into an application. This means, of course, a reduction in the advantages of moving to the cloud, but also ensures easier portability.

Third, 27% of our respondents were developing software on the cloud that could only run on the cloud. These are the firms that are jumping in with both feet and using features of cloud implementation that are not available on premises. These firms are moving toward full cloud in terms both of their software and their culture. These firms are also the ones who are ready to compete with the cloud native firms.

Finally, 26% of respondents indicated they were using the cloud to innovate in other ways beyond just the development of applications. While there are many different ways that cloud can enable innovation (e.g., quantum computing, machine learning), we will talk about two of the more common ways that the cloud enables innovation in financial services: experimentation and business model innovation.

Experimentation and the Cloud

Experimentation and the Cloud

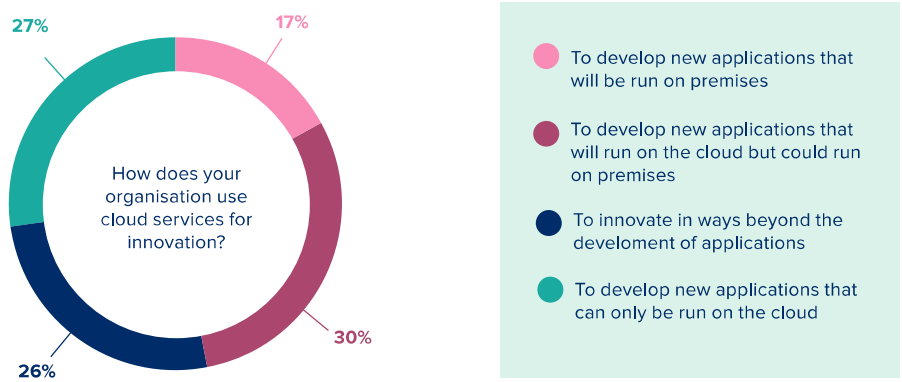


FIGURE. 18

As Stefan Thomke, of Harvard Business School recently wrote, *"whether it's improving customer experiences, trying out new business models, or developing new products and services, even the most experienced managers are often wrong."*[13] His solution: run lots of experiments to test ideas and do so at scale and cheaply. The result is a form of radical incrementalism that creates sustained improvement over time and transforms the value proposition that customers experience, as well as enhancing internal operations exponentially.

> "Banks are fully focusing on cloud adoption. Two of the key drivers are (i) to increase process efficiency and (ii) to reduce operational infrastructure costs. Migrating to the cloud enables banks to capitalise on their ever-growing data treasures in a cost-effective way, implementing data-driven decision making, leveraging the out-of-the-box services provided by hyperscalers. The cloud allows banks to do so whilst maintaining their track record of being probably the industry with highest data privacy and security standards."
>
> Hans-Peter Sailer, Associate Partner, Machine Learning Reply (Germany), May 2021

[13] Experimentation works: The surprising power of business experiments, Thomke, S. H., Harvard Business Press, 2020.

While these experiments can be run in the physical world, the most impressive examples of business experimentation are digital. Companies like Apple, Google, and Booking.com run thousands of experiments every month. They are able to do this because of cloud capabilities that make it straightforward to vary aspects of their offer to customers and then collect and analyse the resulting data. By combining AI, data analytics, and other cloud-based tools, these firms not only slash the cost of experimentation, but make it possible to experiment on aspects of the customer offer that would otherwise be impossible.

This aspect of cloud is not often discussed as a driver for cloud adoption. Yet the value of experimentation over even the medium term is many times the value of potential cost savings or scalability. Of course, to understand and act on the potential of the cloud to support experimentation takes a level of cloud maturity that requires some time to achieve. At the same time, we believe that this aspect of the cloud will receive more and more attention as cloud maturity increases in the finance sector.

The approach adopted by Pictet Group is a good case in point. In 2016, Pictet established Pictet Technologies in Luxembourg, the software factory of the Pictet Group. This team are an accelerator working for the Group's Wealth Management and Asset Management divisions, supporting innovation initiatives and the development of the digital banking solutions of the future. Pictet Technologies leverages the cloud to innovate, to develop and test new applications, even though these applications may eventually run on premises, in line with regulatory requirements and/or the Group's preferences in terms of data privacy and security.

Business Model Innovation

While transforming the way applications are developed and allowing experimentation has huge impacts, it often still means business as usual when it comes to the value provided to customers. But something really interesting happens when a firm becomes full cloud and the organisation starts to think about customer value through the lens of cloud-enabled business. Suddenly, ways to create value for customers that would have been literally unthinkable before the journey to the cloud become opportunities that can be built out quickly into new business, taking advantage of the flexibility and scalability of the cloud. At this point, the firm has become a credible competitor for cloud native firms.

The transformation of MeDirect, a pan-European digital challenger bank with a retail wealth tech platform, is an example of this in action. Around 18 months ago, MeDirect embarked on a cloud first transformation programme to reinvent its business model. The aim was to give customers control over their own investments by becoming their primary destination for personal online financial management. The initiative spanned most business units and teams, requiring a radical shift in how MeDirect operates, generates customer value and drives innovation. MeDirect's IT capabilities are now on par with that of leading fintechs.

In summary, while discussions of cloud often focus on cost effectiveness and scalability, it is increasingly clear that innovation is a key, if not the key, outcome of transitioning to the cloud. While the use of the cloud for software development and testing is well established and easily quantified, there are other, more valuable forms of innovation that accompany cloud adoption once companies reach a more sophisticated level of maturity. The ability to innovate new services for clients and entirely new business models can be transformative for financial services firms. While business cases for these forms of innovation are often challenging to develop, they are nonetheless important strategic outcomes of the transition to the cloud.

Key Leadership Questions on Leveraging the Cloud to Fuel Innovation

The organisations have highlighted how considerations of the benefits of cloud adoption need to move beyond cost effectiveness and scalability. When discussing their firm's transition to the cloud, executives and board members need to include a broad discussion of the effect of cloud adoption on innovation, and the potential for cloud adoption to transform their firm.

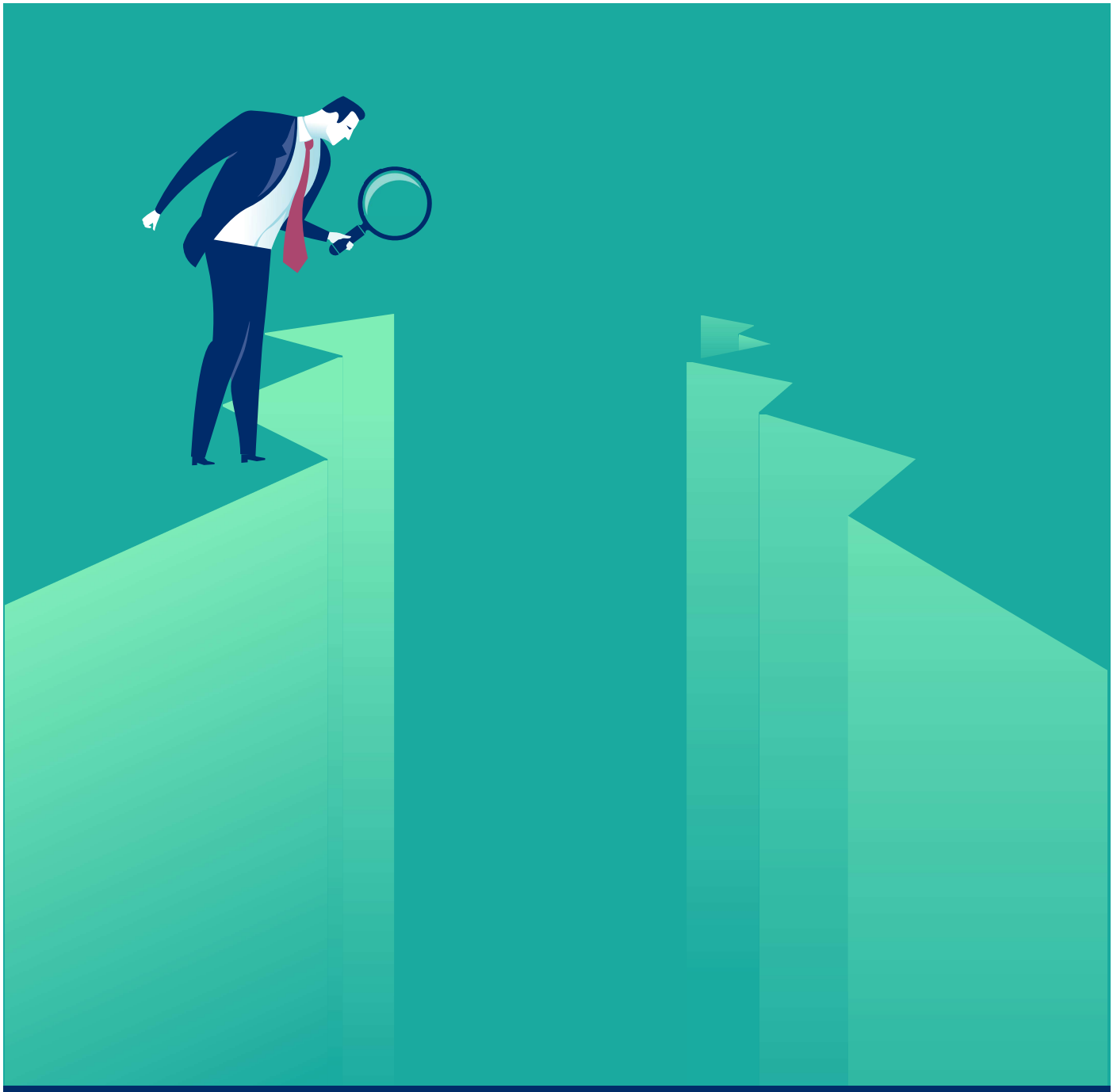
Some of the questions that a financial institution may consider include:

What sort of innovation could the organisation benefit from if it accelerated its transition to the cloud?

- Would adopting cloud speed up and improve software development?
- Would the organisation be able to innovate new services for its clients?
- Would the organisation be able to create new businesses built on new business models?

How important would this innovation be to the organisation?

- Would this additional innovation capability have a significant impact on the future of the organisation?
- How much might this new innovation be worth in terms of cost savings, process improvement, customer retention, and new business?



Section 11

Future Issues

The Green Cloud

The environmental impact of the cloud has become an increasingly common topic of discussion. The complex mining of cryptocurrencies in particular has been scrutinised for the amount of carbon emissions produced, but even the common act of media streaming has been identified as a significant and growing source of greenhouse gases. The connection between cloud services and climate change raises important questions for financial institutions: what is the environmental impact of moving on-premise activity to the cloud? When a firm is striving to be "green", does it make sense to move to the cloud?

One thing that is clear is that moving to the cloud reduces direct energy costs. The use of on-premise computing and data storage require significant amounts of electricity, not to mention the air conditioning systems that are necessary to keep them cool. Moving to the cloud can therefore reduce a firm's energy bills significantly.

This is, of course, good news. But reduced energy consumption on premises does not necessarily mean a reduction in energy consumption overall. Carbon emissions are not about how much a particular user saves, but about the net effect at a system level. It is about whether or not cloud computing reduces the overall carbon footprint of a firm. This begs the question: how "green" is cloud computing?

Drivers of the Green Cloud

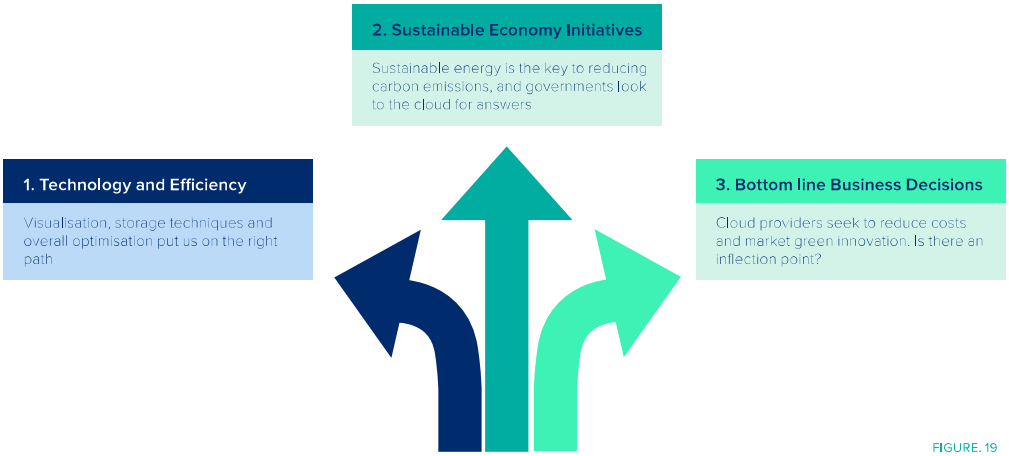


FIGURE. 19

There are three main factors to evaluate when considering this question (See Figure 19 above). First, from a technology and efficiency perspective, there is good evidence that backs the common-sense argument that cloud computing reduces overall energy needs. According to 2020 research published in Science, when comparing data from 2010 and 2018, it was determined that *"global data centre energy use rose to 205 TWh, or around 1% of global electricity consumption. This represents a 6% increase compared with 2010, whereas global data centre compute instances increased by 550% over the same time period."* [14] In other words, a remarkable increase in data centre usage was mitigated by an even more remarkable improvement in efficiency.

The researchers also analysed a scenario in which 2018 computing instance demand was doubled. By factoring in technological advances, such as increased server virtualisation and storage techniques, they determined that energy consumption would increase no more than 1% (see Figure 20 on page 74). So, the dramatic expected increase in data centre usage resulted in only a small increase in energy consumption. This is a strong argument for thinking of the cloud as the green option for computing in financial services.

[14] Recalibrating global data centre energy-use estimates, Science Magazine, February 2020.

Cloud Services Total World Electricity Use[15]

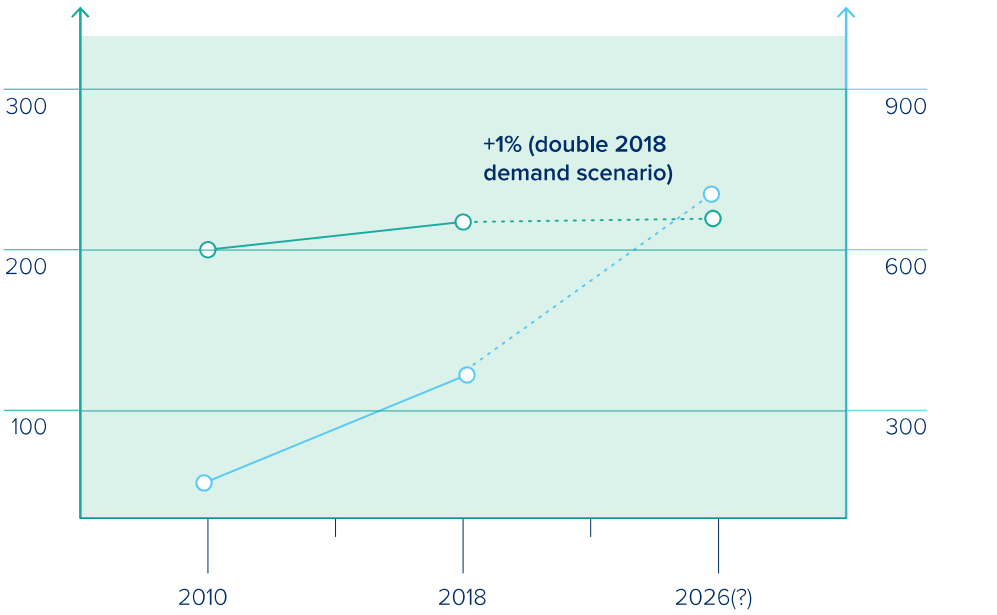


FIGURE. 20

Second, as a component of the Sustainable Economy, the idea of a "Green" cloud seems to be well placed for the foreseeable future, at least in developed nations. For example, the European Union's highly touted "Green Deal" includes a heavy focus on the importance of technology in the race to effectively reduce carbon emissions. The deal describes several to-dos, among which is to *"explore measures to ensure that digital technologies such as artificial intelligence, 5G, cloud and edge computing and the internet of things can accelerate and maximise the impact of policies to deal with climate change and protect the environment."* [16]

In addition, major infrastructure initiatives to steer economies towards Paris Agreement goals promise to play a major role. In December 2020, the Biden administration in the U.S. released an outline of its plan to eliminate carbon emissions from the national electric grid by 2035, effectively ensuring that cloud service providers in the U.S. will be supplied green energy to run their services. This focus on providing green energy to the cloud provides a simple but dramatic way to reduce the carbon emissions from the computing and storage activities of thousands of companies.

Third, what is good for the environment is also what is good for the bottom line of cloud service providers. In addition to moving to green energy, cloud service providers are motivated to reduce energy usage as much as possible as this is one of their main costs. This fact has brought us some innovative examples of providers experimenting with radical ways of reducing energy costs, such as Microsoft's self-cooled underwater data centre. While these green innovations are sometimes perceived primarily as a marketing exercise, they are evidence of the cloud service providers' attempts to reduce energy usage.

At the same time, while publicly-traded cloud service providers may feel particular pressure from green minded investors to reduce energy consumption, how can we be sure that these providers will always make choices that are in the best interests of the environment? Cloud service providers can place their data centres in any location on earth (or space!). It is not difficult to imagine cloud infrastructure physically located under the jurisdiction of a government with favourable tax / business incentives, though comparatively lax energy standards. Potentially high profit margins for this hypothetical cloud provider may convince them to see the environmental consequences as a necessary evil and a viable trade off.

[15] Recalibrating global data centre energy-use estimates, Science Magazine, February 2020.

[16] The European Green Deal, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, December 2019.

Putting all this together, while the environmental advantages of the cloud have so far not been an important driver for adoption in our survey or in the interviews we conducted, this is likely to change in the future. As financial institutions come under increasing pressure to reduce their carbon footprints, and as the large cloud service providers become greener, we believe this will increasingly become a key driver accelerating and deepening the move to the cloud. It is also therefore likely to become an increasingly important criterion used by firms in the selection of their cloud service provider, as highlighted by the panel members from leading global financial institutions speaking at the Reply Xchange session on Cloud in Financial Services held in June 2021.[17]

> "With the cloud, you are only consuming the power when you need to; you are consuming the power in an efficient way; and the power that you are consuming can be delivered from very green sources. It is an advantage that we are going to investigate more and leverage more."
>
> Ian Haynes, Head of Cloud Services, HSBC, June 2021

Cloud-based Quantum Computing

Quantum computing refers to processors which follow the laws of quantum mechanics, or rather the physics of the smallest dimensions of nature where physical phenomena like superposition and entanglement arise. Through advances in technological know-how, these phenomena can be harnessed to perform extremely complex computations, some of which are considered impossible with traditional computers.

> "With increased access to quantum computing via the cloud, and with the quantum hardware race under way, financial institutions may find concrete uses for quantum computing in the coming years to solve many complex problems in a better and faster way."
>
> Marco Magagnini, Partner, Leader of Reply's Global Quantum Computing Practice, May 2021

Maintaining a quantum computer in an adequate environment is no easy task. In fact, it is exceptionally rare for an organisation to actually host quantum computing hardware. This is where the cloud comes into play: connecting to quantum computers over the cloud is the most viable (and scalable) solution for users to access quantum devices and their powerful resources.

The advent of cloud-based quantum computing has enabled the application of this technology in many ways and in many sectors. All quantum computing use cases have a common factor: performing complex calculations as quickly as possible. By accessing Quantum Processing Units (QPUs) over the cloud, machine learning algorithms and Monte Carlo simulations are greatly enhanced, which has helped solve workforce management optimisation problems in the energy sector[18], for example.

[17] A recording of the session, Never waste a good crisis: The challenges of rapid Cloud adoption in Financial Services, is available at https://xchange.reply.com/.

[18] https://www.reply.com/data-reply/en/stories/quantum-algorithms-for-the-optimization-of-maintenance-work

In financial services, where the proverb “time is money” is commonly applied, ironically, cloud-based quantum computing has been given relatively little importance so far. According to our survey (see Figure 21), quantum computing will be the least important cloud-related strategic focus (for both IT and Business) over the next three years. This survey response may be a reflection of the current limits of quantum computing’s uses to highly specialised financial institutions or to specialised areas of financial services, such as the optimisation of daily collateral costs related to over-the-counter derivatives trading.[19]

What is your Organisation’s Strategic Focus (for both IT and Business) related to the Cloud for the next three Years?

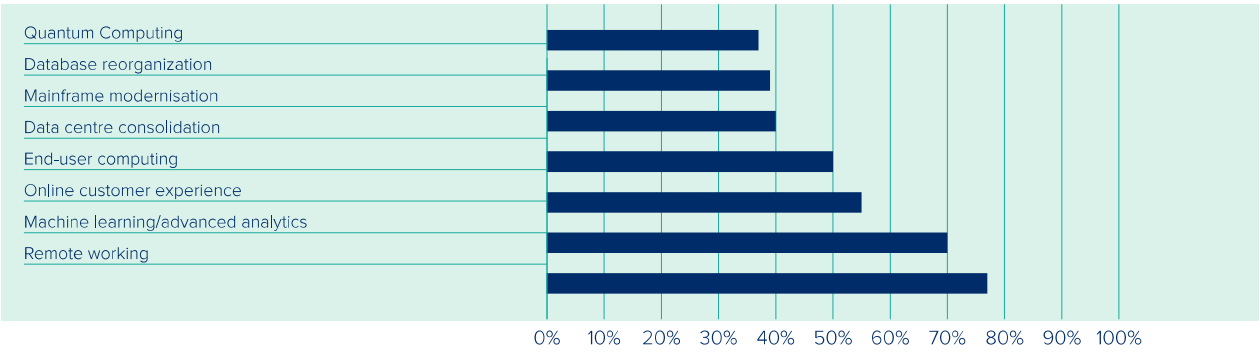


FIGURE. 21

Based on 154 valid responses to the Imperial College Business School & Reply Cloud in Financial Services Survey (February 2021). Respondents to the survey were asked to rate each item given on a scale from 1 (not relevant at all) to 5 (extremely relevant). For example, remote working was selected as "relevant" or "extremely relevant" by 77% of our respondents, while quantum computing was selected as “relevant" or "extremely relevant” only by 37% of our respondents.

However, beyond derivatives, the typical financial institution requires an enormous amount of computational power to processes its daily lot of problem-solving activities. Looking forward, this is why we view financial services as the perfect playground for quantum technologies to speed up calculations: from the development of market forecasts, to simulating asset prices, to what-if market scenario, and stress tests, cloud-based quantum computing may save users time, and therefore money.

Will increased access to quantum computing technology via the cloud progressively change the opinion of financial services decision makers in the near future? As its uses are shifted to solving to more common problems, we may see a shift in strategic focus.

[19] https://www.reply.com/en/topics/quantum-computing/qubo-quantum-inspired-algorithm

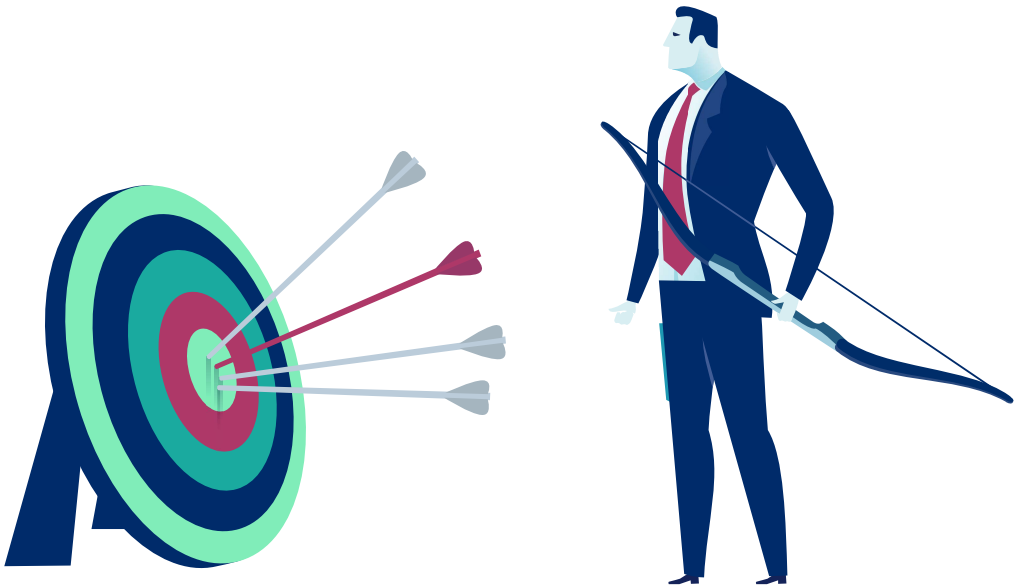
Conclusion

Board rooms and the C-Suite have had to get to grips with repeated major technology shifts that have disrupted their businesses – the advent of the personal computer, the internet & eCommerce, smart phones and mobile computing. The cloud represents another of these seismic changes with profound ramifications for business.

Leaders of financial institutions must think through how the emergence of hyperscalers (Amazon Web Services, Microsoft Azure, Google Cloud...) will impact their business, customers, supply chains, employees and, perhaps most importantly, existing and emerging competitors. The disruption – think Netflix and broadcast media, Spotify and the music industry, Uber and mass transportation, Amazon and retail, the eponymous Zoom of the pandemic remote working experience, the fintech start-ups and challengers to name a few – will continue to accelerate. As businesses digitise, the cloud is, and will be, a fundamental enabler of this disruption.

As our research and survey have confirmed, cloud services are here to stay in financial services. Each financial institution is at a different point on its journey to the cloud, and the choices it makes should be dictated by the strategic objectives it is pursuing and the challenges that the institution faces. Firms need to be strategic in their adoption and there are important questions that need to be addressed as they move more and more activity to the cloud. While some of the problems are technical, this report highlights that there are significant strategic and organisational challenges that need to be dealt with in the Board room and the C-suite to ensure cloud adoption is successful and that firms derive maximum value from the move.

Last but not least, the cloud of today is not an `end-state'... As our research and survey have confirmed, a financial institution's cloud strategy needs to be about more than ownership of the servers and whether an application runs on premises, or on a private, public or even hybrid cloud environment. But it also needs to be revisited as the technology evolves to ensure that the choices of today still hold true tomorrow.



Reply specialises in the design and implementation of solutions based on new communication channels and digital media. As a network of highly specialised companies, Reply defines and develops business models enabled by the new models of AI, big data, cloud computing, digital media and the internet of things. Reply delivers consulting, system integration and digital services to organisations across the telecom and media; industry and services; banking and insurance; and public sectors.

www.reply.com