University of Strathclyde Glasgow

University of Glasgow

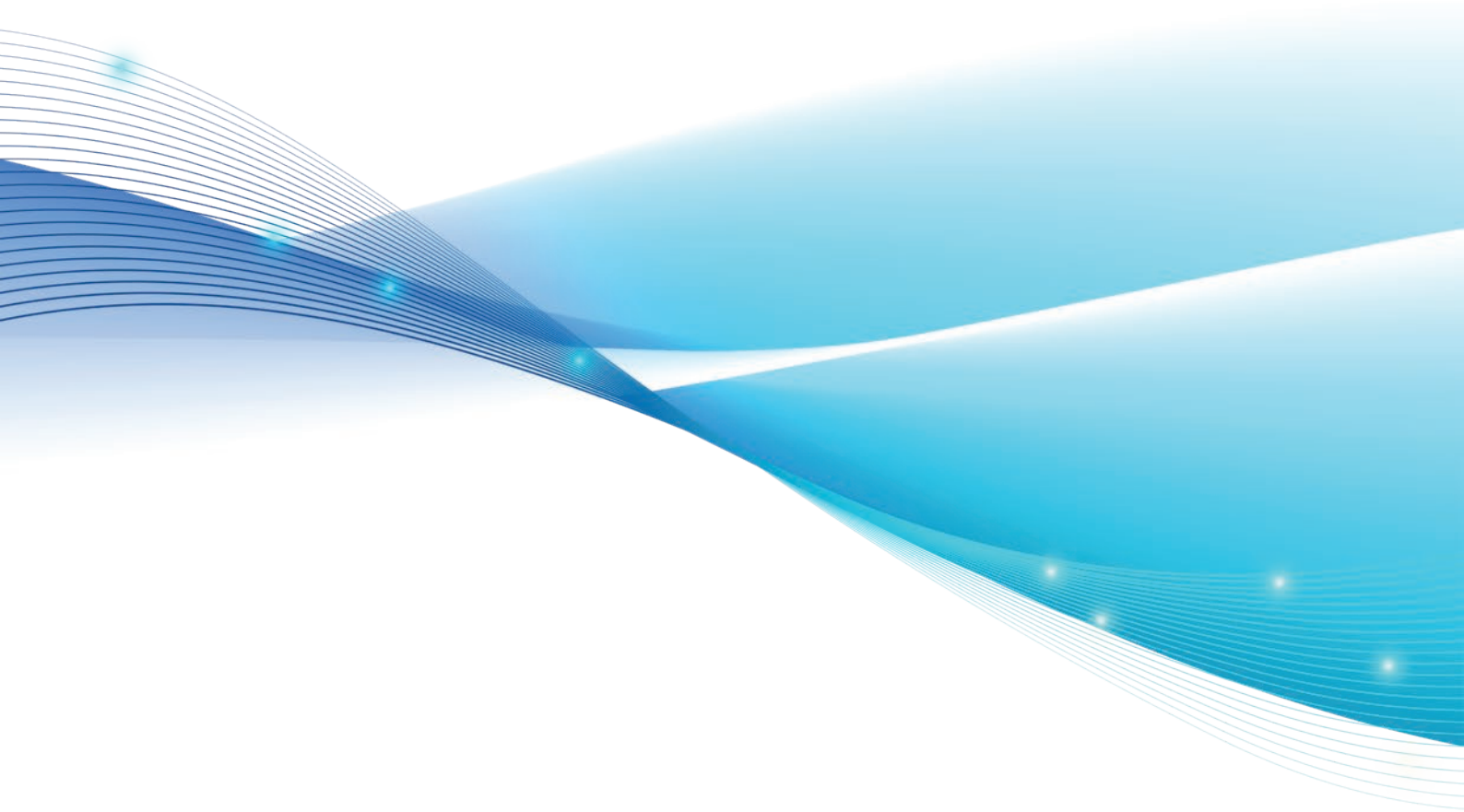
FinTech Scotland

Pinsent Masons

Cloud for financial services

An Industry Report on the Opportunities and Challenges

By Pinsent Masons & the Financial Regulation Innovation Lab (FRIL)



A PURPOSE-LED PROFESSIONAL SERVICES BUSINESS
WITH LAW AT THE CORE

CONTENTS

Pinsent Masons is an international law firm. We help our financial services clients navigate technology changes and challenges. We act as a change enabler, empowering organisations to form lasting strategic alliances, underpinned by robust legal and regulatory frameworks that support their commercial objectives.

FRIL is an industry-led collaborative research and innovation programme focused on leveraging new technologies to respond to, shape and help evolve the future regulatory landscape in the UK and globally.

Introduction

In 2016, Pinsent Masons led a banking sector-wide collaboration and published a report titled "Banking on Cloud". It identified seven key hurdles to cloud adoption for financial services businesses, ranging from regulatory uncertainty over what constitutes a "critical or important" function to the practicalities of supply chain oversight and data residency. At the time, the conversation was dominated by caution, risk mitigation, and the challenge of fitting a transformative and not-widely adopted technology into a traditional outsourcing framework.

Almost a decade later, the landscape has fundamentally changed. The discussion is no longer about *if* financial institutions should adopt cloud, but *how* they can leverage it as a cornerstone of their strategic future. The journey has been neither simple nor linear. The early, simplistic mantras of "cloud first" have given way to a more nuanced and mature strategy of "cloud appropriate," integrated within a broader, and more urgent, modernisation agenda where legacy technology weighs heavy.

The regulatory landscape has also undergone a significant shift. The initial guidance from the Financial Conduct Authority (FCA) was soon supplemented by detailed guidelines from the European Supervisory Authorities[1]. While the UK was part of the EU, the financial services sector had to comply with these new, detailed requirements. Post-Brexit, the Prudential Regulation Authority (PRA) issued Supervisory Statement SS2/21, which established a comprehensive framework for outsourcing and broader third-party risk management, imposing requirements that, in many respects, paralleled the EBA's guidelines, including cloud-specific ones, but with a UK focus.

The most significant development, however, may be the EU's Digital Operational Resilience Act (DORA), which came into force in January 2025. DORA represents the most comprehensive regulatory framework for digital resilience in financial services globally.

DORA introduces prescriptive legally binding requirements with technical standards for ICT risk management, incident reporting, and third-party risk management and also sets out a direct oversight regime for critical third-party service providers (CTPs). In parallel to DORA, a significant number of other operational resilience and third-party risk regulatory frameworks have been enacted which have an impact on cloud adoption. This general shift to prescriptive regulation has changed how financial institutions approach their reliance on technology.

This report revisits the cloud journey for financial services with a focus on the nuanced and complex reality facing financial institutions. Drawing on a series of candid "Chatham House" interviews with senior leaders across major financial institutions, technology providers, and advisory firms, we explore the current dynamics of the market. Our report is also supported by survey data which we sourced from 30+ businesses operating within the financial services sector.

The interviews and the data reveal that the old hurdles have not disappeared, and some, like data residency, persist as challenges despite the context evolving. The primary drivers for moving to cloud are now strategic – the (1) continuing need to escape the drag of legacy systems, (2) demand for pace and agility in segments being reshaped by AI, and (3) realisation that cloud can be a powerful tool for enhancing, rather than diminishing, operational resilience.

New and complex challenges have also surfaced. The initial promise of cost savings has proven elusive for some, governance and the maturity of shared responsibility models have struggled to keep pace with adoption, and regulators are focused on what they see as a continuing key concern – concentration of risk among a handful of hyperscale providers.

As we stand on the cusp of an AI-powered technological wave, a wave which is dependent on cloud, the lessons from the past decade are more critical than ever.

Almost a decade later, the landscape has fundamentally changed. The discussion is no longer about *if* financial institutions should adopt cloud, but *how* they can leverage it as a cornerstone of their strategic future.

[1] The European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) collectively form the ESAs.

A decade of change: revisiting the old hurdles

In 2016 a group of senior leaders in financial institutions identified the key 7 challenges to cloud adoption in the financial services sector. In this section, nine years on we revisit each of these challenges.

1. Clarifying what comprises a 'critical' function:

The debate has matured from definition to implementation, with regulatory frameworks, including DORA, necessitating registers of information which require clear classifications of third-party services. Classification overlaps and inconsistencies however, persist with 'new' operational resilience categories such as 'important business services' not always fully aligning with the shift in third-party risk management, which is moving away from outsourcing and towards governance of relationships with all third-party service providers.

2. Supply chain oversight:

This remains a critical challenge and is now amplified by hidden concentration risks and a regulatory focus on fourth-party risks and beyond. The rules are now more prescriptive than they were in 2016 and standardised approaches towards dealing with them have also emerged. Regulators have moved towards expecting regulated financial entities to acquire a comprehensive understanding of their entire service delivery chains. Contractual mechanisms to support this, the requirement for providers to flow down obligations to their subcontractors have become more defined and have increased.

3. Enabling regulatory oversight & access:

The focus has shifted decisively from debates over physical data centre access to direct regulatory supervision of the vendors themselves under CTP supervisory regimes. The significance and impact of this new era of direct powers over systemically important technology providers remains to be seen as it develops over the coming few years.

4. Managing cloud-specific risks:

In 2016, there was no regulatory framework which applied to operational resilience nor was there clarity on what constituted "undue risk" or even more broadly "operational risk" from a regulatory perspective. In the years since, this has changed dramatically with detailed operational resilience frameworks coming into force in the UK and elsewhere. With these new frameworks in place, cloud has in many respects evolved to be seen as a means of enhancing operational resilience with approaches to disaster recovery, business continuity, security and vulnerability management accommodating sector-specific requirements.

5. Data location:

Data residency remains a persistent and complex compliance challenge for global institutions. While standardised approaches address many of the issues, as new ones come to the surface the challenge remains.

6. Data management & breach reporting:

Standardised and stringent breach notification rules and incident response approaches have become business-as-usual despite their often high-risk setting, though harmonisation remains imperfect. DORA has introduced a new regime which has again required significant adjustments to be made.

7. Termination & exit:

The challenge of vendor lock-in has intensified while regulators now demand detailed, credible, and tested exit plans for critical and important arrangements. The early promise of portability has largely gone unfulfilled, according to some of our interviewees.

1. Strategic drivers for cloud in financial services

The business case for cloud has matured significantly. What began as a conversation about cost and efficiency, enabling long-held (often in-house) capital heavy data centre equipment to be decommissioned, has evolved into a sophisticated set of strategic imperatives that are reshaping the core operations and competitive posture of financial institutions.

1.1 From 'cloud first' to strategic modernisation

The early industry mantra of "cloud first," which saw some firms adopt the technology with more enthusiasm than strategy, is now viewed as an overly simplistic, and sometimes flawed, approach. As one senior leader at a global bank reflected, "In retrospect, going cloud first exclusively was probably not the right call". A key reason for this reassessment was a miscalculation of the financial implications, as the same leader noted, "one thing that was massively under factored for at that point was the cost involved with cloud."

The strategic focus has now pivoted from a pure cloud-centric push towards a more holistic modernisation agenda. The goal now is to achieve a "where it's appropriate to use cloud" model. Within this new framework, cloud is a critical pillar, but the primary driver is addressing the immense operational and financial drag of outdated systems.

One interviewee noted that most large institutions "still have a substantial, let's call it what it is, mainframe legacy of capability in their organisations". A leader from a Big Four firm concurred, highlighting that financial services firms have "complex legacy estates in IT" and that the associated transition is "very difficult to unwind".

The true impetus for modernisation is the realisation that the "biggest suction on cost for the organisation was actually all the legacy infrastructure". This modernisation effort is also supported by the financial benefits of shifting expenditure from capital investment (CapEx) to operational spending (OpEx), which can provide greater balance sheet flexibility.

This is a long-term endeavour. As one interviewee on behalf of a bank put it: "we're on that modernisation journey now and we will probably be for 10 years".

1.2 Pace, agility and competitive advantage

While cost savings may have been an initial driver for some, the demand for speed and agility has proven to be a core, enduring benefit of cloud. A key theme from our interviews was the focus on acceleration.

Cloud platforms provide an unparalleled ability to experiment and deploy new capabilities rapidly. In the words of one technology executive, "You can very quickly bolt new stuff in if you're in that cloud environment where it's far harder to do otherwise".

This agility is no longer a 'nice-to-have'; it is a critical source of competitive advantage. The true value lies in the "immediacy of access to the next versions" of cutting-edge technology.

As one expert explained, the ability to "switch to the next version of ChatGPT or Claude or whatever the model might be and then immediately being able to exploit those new capabilities is where the cloud advantage comes from. You just get access far faster". This provides a "competitive advantage that you just can't match for pace."

1.3 The strategic shift from build to buy

The imperative for speed has also driven a cultural and strategic shift away from traditional 'build' mentalities. Historically, firms in some financial services sub-sectors derived their "edge from highly customised, highly bespoke technology that wasn't replicable easily." The downside of this approach was the need for "highly, highly specialised technologists" and the difficulty in tapping into the broader industry talent pool.

In the early 2020s this was beginning to be recognised as a "poor way to take advantage of the talent pool in the industry." A conscious switch was made, based on the philosophy that firms "don't need to have unique and bespoke technology to get a commercial advantage. Instead, we should be moving to industry standard technologies."

1.4 Enhancing operational resilience

Perhaps one of the most significant shifts in perception over the last decade relates to security and resilience. In 2016, the perceived security risks of the cloud were a primary barrier to adoption. Today, leveraging the scale and specialisation of hyperscale cloud providers is increasingly seen as a way to enhance resilience.

The concept of operational resilience enables firms to "learn cross industry and think more in terms of a general set of principles" which improves sector resilience overall. "Resilience comes at a price, however, particularly when your critical cloud environments are being replicated across multiple local DCs [data centres] and then also multi-region", as one interviewee put it.

This has transformed the challenge of physical security to managing the complexities of the cloud operating model. Mastering the "shared responsibility model" has been a major focus, with one leader admitting that clarity over ownership of responsibility "wasn't always clearly mapped out."

Similarly, managing vulnerabilities in a hybrid environment requires new processes: "is it part of your on-prem vulnerability management process or is it unique to cloud". For others, the journey to get these fundamentals right has been a steep learning curve and they are "really only coming out the back end of that now coming into 2025."

Regulatory implications of operational resilience

According to the PRA, the use of cloud can benefit a firm's operational resilience. In SS2/21 the PRA affirms that cloud use "can strengthen firms' ability to respond and recover from local operational outages faster and more effectively and enhance their ability to cope with fluctuations in demand." However, the PRA is also unequivocal in its expectation that regulatory accountability is not transferable to cloud service providers.

While the PRA recognises that the shared responsibility model means that from a technical perspective the cloud service provider is responsible "for the provision of the cloud" while the firm is responsible for "what's in the cloud", firms must mitigate the risks of potential regulatory failures regardless of whether they are technically responsible in the first instance. If a cloud service failure leads to a breach of a firm's defined impact tolerances for an important business service, the PRA, and the FCA through its parallel SYSC 15A requirements, will hold the firm, and not the cloud provider, accountable and exposed to fines, senior manager sanctions and potential directions against the business as a whole.

> **When a business gets unexpected and sometimes wild results from a model, it's often because of what it fed it. This is compelling organisations to finally undertake the "hard, boring bit of sorting the data out" and invest in building "gold standard data sources".**

1.5 Unlocking data for AI

The emergence of AI is a new strategic driver for cloud adoption. The two are inextricably linked. As multiple interviewees stated, "Cloud will be fundamentally part of the Gen AI journey", and for most firms looking to leverage AI, they "don't have any choice and have to go to the cloud because they probably don't have the cash" to build the required infrastructure themselves.

The AI ecosystem itself is cloud-native. When "…engaging third party vendors which have Gen AI capabilities, those vendors are all cloud based" and so firms can often be left with no choice but to move with the technology or face being left behind.

However, the push towards AI has cast a harsh light on the long-standing, unresolved issue of data quality. As one expert put it, "Legacy data is not AI-friendly." Poor data quality is an "everything problem," but "AI just makes it really obvious."

When a business gets unexpected and sometimes wild results from a model, it's often because of what it fed it. This is compelling organisations to finally undertake the "hard, boring bit of sorting the data out" and invest in building "gold standard data sources." Only then will firms be able to maximise the potential benefits of leveraging AI from cloud resources.

Contractual approaches which enhance operational resilience in a cloud context

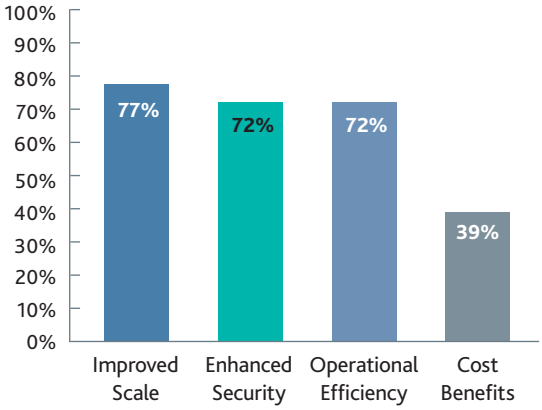
In a contractual setting, firms need to consider how best to address their need to meet impact tolerances. In many cases a generic service level agreement may not suffice and the business may need visibility into specific recovery time objectives (RTOs) and recovery point objectives (RPOs) to ensure that there is no regulatory gap.

Firms may also need to think about whether their cloud service providers will be required to support scenario testing exercises and their need to simulate severe but plausible events that have an impact across the supply chain. Orderly exits and transfers, data locations and communication and information sharing requirements in relation to business continuity and vulnerability management should also be carefully considered when contracting.

Data Insights: Results from our industry survey

To validate and enrich the insights for this report, we surveyed a cross-section of senior leaders in financial services about the benefits, barriers, and strategic realities of cloud adoption.

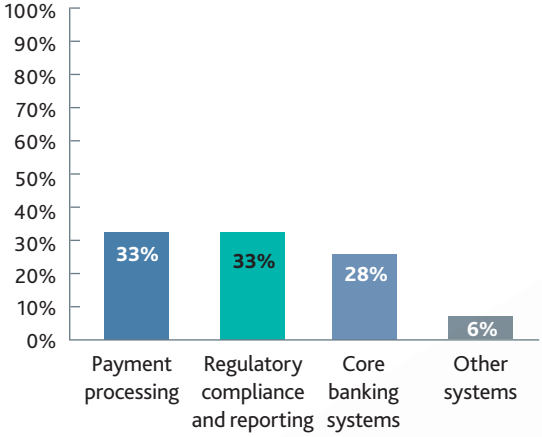
The primacy of strategic benefits over cost



When asked about the benefits of cloud adoption, respondents overwhelmingly prioritised strategic and operational enhancements over simple cost savings. Respondents were asked to rate a list of potential cloud benefits on a scale of 1 to 5 with 1 representing "unimportant", 4 "important" and 5 "very important". The data reveals that:

- **Improved scale** was a standout benefit, with a total of **77%** of respondents rating it as either important or very important
- **Enhanced security** and **operational efficiency** were also seen as critical, with both scoring **72%** in the aggregated important or very important category
- Conversely, **cost benefits** were a point of division, with only **39%** viewing them as important or very important, while **33%** rated cost benefits as unimportant

Strategic hesitation: core systems remain a red line for some



While adoption is broad, there is still significant reluctance to migrate the most critical core functions. When asked which areas respondents were most hesitant to move to cloud, the top answers were:

- **Payment processing** (33% reluctant)
- **Regulatory compliance and reporting** (33% reluctant)
- **Core banking systems** (28% reluctant)
- **Other systems** (6%)

2. Current and continuing challenges

Despite clear strategic benefits and widespread adoption, the path to cloud maturity is not without challenge. The current challenges are often less about the technology and more about the complexities of governance, cost management, regulatory engagement, and organisational culture.

2.1 The governance gap: building the plane while it's flying

A recurring theme is that technology adoption has frequently outpaced the development of robust internal governance. In the rush to meet business demands, many institutions "didn't necessarily spend sufficient time getting the governance structures, the underlying infrastructure and the control that the infrastructure requires in place first." This has led to a situation frequently described as "building the plane while it's flying."

One interviewee explained the dynamic: "you're flying at the same time you're trying to build all your controls… never really got a chance to prepare and say here are the types of controls we should build, then build them and then you can start adopting." This governance gap is a primary cause of regulatory findings and engagement, where robust governance is too often seen as a "nice to have rather than a fundamental underpinning of how to do it well at scale."

2.2 Cost: The myth of automatic savings

The initial belief that cloud would automatically deliver significant cost savings, a key driver in the 2016 report, has diminished. One interviewee indicated that after initial adoption, "any reference to cost savings disappeared from the strategic documentation." The financial reality is far more complex and initial savings may erode over time as dependencies deepen, and vendor pricing models evolve.

A further primary reason for less emphasis on cost savings is the reality that during long transitions, firms are often "still carrying the legacy infrastructure", while also paying for new cloud services. As a Big Four consultant noted, "financial institutions are not start-ups; they have legacies."

The emergence of AI has added another layer of unpredictability, with one interviewee warning that with AI workloads, the long-term economic consequences are not always considered at the outset. It can be "very, very easy" to move forward with a specific use case without understanding that it could lead to "a massive bill and no real end result."

2.3 Dealing with regulators: "the importance of telling the story"

Understanding of the importance of cloud by the regulators themselves has undergone a significant change since 2016. By 2018 there was a noticeable shift in view of the importance of cloud for financial services. "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", said a Future of Finance report commissioned by the Bank of England.

The Bank of England itself also responded positively, asserting that it "recognises the potential cyber and operational benefits cloud-based models can bring, particularly for smaller firms."

This is not the only example of regulators shifting their view to one of understanding the need to enable the use of cloud across the financial services sector. The FCA, with an intent of balancing the benefits of cloud against the risks, stated in its 2025 strategy for retail banks that it recognises "Banks' transformative changes now typically involve migration of banking and mortgage platforms to public and/or private cloud."

While the relationship with regulators has matured, a persistent challenge for regulated firms is how to effectively communicate compliance. As one executive admitted, "We're not good at telling the story when we get asked by a regulator."

A common pitfall is a reactive approach to demonstrating internal firm processes. When regulators ask for evidence of compliance, the response can be to "create this slide pack to explain to the regulator what we're doing instead of let's just show them our process flow." This lack of embedded, easily presentable documentation fails to give regulators confidence, even when the underlying controls are sound.

Nevertheless, the focus of regulators remains on the fundamentals including "change management, identity and access management, and the interface controls." The cloud service providers who have understood this have gained a significant advantage. According to one bank, some providers have lagged behind others because they initially did not prioritise these "regulatory sensitivity" issues to the same degree, and this has been reflected in market-share.

For those cloud service providers that have recognised the importance of regulatory sensitivity in the financial services sector, this has led to an evolution from the imposition of standard form contracts to embracing the use of addendums specifically designed for the financial services sector. This approach has seen leading cloud providers address many of the issues which were key concerns 10 years ago – broad access and audit rights to satisfy the demands for effective regulatory oversight, commitments on service and data locations and security and assurances regarding oversight of the supply chain.

That is not to say however that no challenges remain. For retail banks, for example, the growing expectation that the dual impact of new operational resilience requirements and the Consumer Duty has brought the need to prepare effective exit strategies to the fore.

Understanding of the importance of cloud by the regulators themselves has undergone a significant change since 2016.

For market infrastructure providers, this emphasis has been even more pronounced, with a clear expectation from regulators that providers demonstrate their ability to ensure their resilience in a manner that protects against systemic risks that could have an impact on the broader financial system.

2.4 Organisational and culture: people as the barrier

Ultimately, the greatest barriers to successful cloud adoption are often human, not technological. A "big disconnect between the business and IT" can lead to a lack of progress where teams fall into "that bad habit [of] doing separate things and then one can blame the other." One interviewee observed that some "in-house technology teams are protective of their work and ability to manage complex legacy estate." This is compounded by change fatigue, as "many financial services colleagues have been through considerable change management" already, which can impact their appetite for a major cloud transition.

Risk aversion is of course a fundamental aspect of the culture, shaped largely by the regulatory landscape in which financial institutions operate. This context has led to cautious mindsets and a strong preference for established procedures that have proven effective in managing risk over time.

It has also meant that reliance on familiar systems has resulted in hesitation in adopting cloud services. Such caution may stem from a combination of psychological and practical concerns. These concerns are further intensified by skill gaps, as many professionals feel ill-equipped to navigate unfamiliar systems and worry about their ability to adapt to rapid technological change. Overcoming these issues requires engagement at the highest levels, as another interviewee noted "unless we can have a conversation with the right people across the business… we're just going to get stuck."

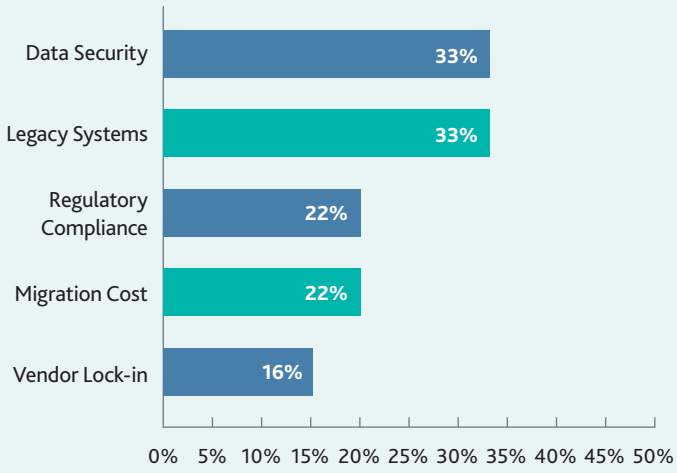
Barriers: From blockers to navigable challenges

In a clear sign of the maturity of the sector, perceived barriers to adoption scored significantly lower than benefits. The data suggests that while challenges exist, they are no longer seen as insurmountable blockers.

Issues often cited as major hurdles such as **regulatory compliance concerns**, **vendor lock-in**, and the **cost of migration** received lower scores. This indicates the continued importance of data security and legacy systems as the front of mind issues.

Barriers: From blockers to navigable challenges

Respondents were asked to rate a list of potential barriers to using cloud on a scale of 1 to 5 with 1 representing "unimportant", 4 "important" and 5 "very important". The chart below sets out the total percentage of respondents which certain barriers as either important or very important:

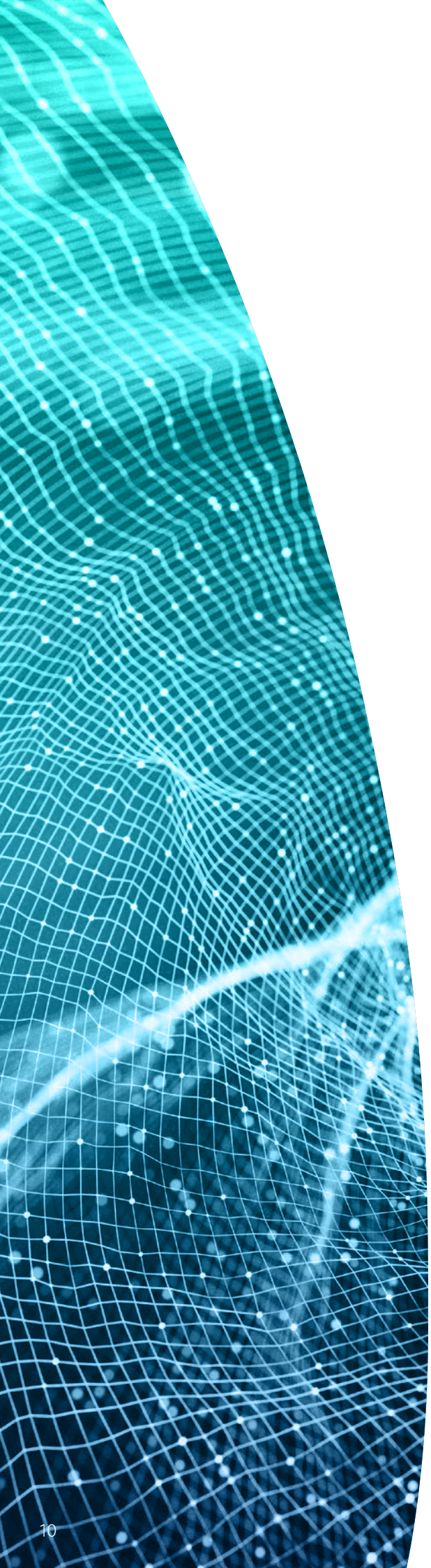


2.5 Persistent data challenges

Data management remains a central and multi-faceted challenge, echoing many of the concerns from 2016. Four key areas that continue to stand out are:

- Data security
- Legacy data
- Data residency
- Reputational risk

> **Risk aversion is of course a fundamental aspect of the culture, shaped largely by the regulatory landscape in which financial instituitions operate.**



Data Security
The focus has shifted to the nuances of the cloud environment. This includes: managing the network perimeter; the complexitities of the shared responsibility where ownership "wasn't always clearly mapped out"; and dealing with vendor terms that can be problematic, such as those that "won't accept any liability for loss" of client data.

Legacy Data Curation
This has become a critical prerequisite for unlocking the value of AI. There is a tendency for businesses to "want to leap to the end" without addressing legacy data issues. Yet, as one interviewee stated, "data quality is always the issue" and most organisations face a "massive data quality and integrity challenge."

Data Residency
This was a major hurdle in 2016 and, according to one senior banker, it is still "not solved." Data localisation requirements remain "massive." For global firms, navigating the requirements of different regulators, particularly in Asia where they "each have their own kind of nuances," is a persistent operational challenge.

Reputational Risk
The fear of a major public failure looms large. High-profile incidents, such as bank migrations which left customers unable to access their accounts for days, serve as a powerful cautionary tale and a significant inhibitor of risk appetite.

2.6 Third-party risk and supply chain visibility

Ensuring oversight of the supply chain was Hurdle 2 in our 2016 report, and the challenge has only intensified. Assessing fourth-party (and beyond) risk is described as "incredibly difficult, time consuming, expensive."

Historically, vendors have been poor at providing transparency into their own supply chains, a weakness continually exposed by high-profile incidents, such as the recent Crowdstrike outage, which are forcing the issue up the agenda.

This creates a "fragmentation risk" where a firm has handed out its value chain to third parties, and it "only takes one part of the chain to make an error" for the firm to suffer detriment. For some, the sector continues to be seen as "grappling and evolving, but not there yet in terms of that total connectivity."

The UK requirements evolved significantly with SS2/21 setting out in detail supply chain visibility requirements. Those requirements include obligations to involve fourth-party suppliers in the "severe but plausible scenarios" that firms test to prepare for potential failures or disruptions.

In the EU, DORA has introduced a detailed regulatory technical standard which focuses solely on subcontracting and sets out the protections which should be in place to ensure sufficient visibility. It requires regulated entities to meet prescriptive due diligence and pre-contractual risk assessment requirements, conditions for subcontracting and include specific contractual protections to manage material changes to subcontracting arrangements and termination.

3. Vendor dynamics

The relationship between financial institutions and the small number of hyperscale cloud providers is a critical and evolving dynamic, characterised by deep dependency, strategic risk, and increasing regulatory scrutiny. This, however, is only one side of the market, with financial institutions also needing to understand and assess how best to integrate low risk cloud-based service providers that sit within the technology stack.

3.1 Vendor lock-in and the exit strategy challenge

As one leader described it, the risk of "developing dependency on one vendor, with very high switching costs" is a primary concern for financial institutions. For smaller firms, this is often exacerbated by free service offerings which the firm comes to rely on, only to find the risk that the provider can "just turn these services off" or increase costs substantially such that the solution becomes unsustainable.

This dynamic makes exit planning, a key regulatory requirement and Hurdle 7 in our 2016 report, extremely challenging, as some believe that the initial promise of application portability has largely failed to materialise. As one interviewee stated, the idea was that "if you build an app in a certain way you can run it in this way and then move it around more. None of that happens." Further, as firms consolidate systems onto single platforms, combining software as a service and platform as a service, to achieve a "perfect data trail," they are simultaneously "making it more difficult to move".

3.2 Concentration risk

The market's reliance on a few dominant cloud providers creates concerns around systemic or concentration risk, according to the regulators, which need to be continuously assessed. While firms are aware of this, the practical solutions are limited.

The theory of maintaining a "hot standby on another cloud" is often financially unviable, as one interviewee noted: "we would spend all our money on operational resilience." While concentration risk is "talked about, its approved, diligence signed off," it remains a persistent challenge that "continually needs to be on agenda" with no clear strategy to tackle the issue.

The issue extends beyond a firm's direct suppliers to the indirect dependencies throughout the technology supply chain. Firms need to think not only about their direct suppliers, but also about who those suppliers depend on.

The message to regulated entities, however, is clear – there is a need to manage concentration risk through "reasonable steps" which means not just due diligence exercises but also robust contractual protections. Firms that have not met the regulatory standards for business continuity plans, testing, remediation and root cause analyses are likely to place themselves in the regulatory spotlight in circumstances where the regulator, on review of its own data, concludes that an unacceptable concentration of third-party dependence exists. Where exit strategies are also not effective in concentrated scenarios, there is an even greater likelihood for regulatory action.

3.3 Regulatory overhead as a barrier for new entrants

The heavy regulatory frameworks in financial services are perceived to create a significant barrier to entry for smaller, innovative cloud providers. One risk leader observed that small providers find it "really difficult" to keep up with the weight of regulatory requirements.

The industry's "heavy duty" frameworks demand "significant docs and technical information they may not have," which "rules them out of getting a contract sometimes" and reinforces the dominance of the "bigger players instead". Whilst there is a clear need for regulatory governance to ensure data and process security, this has been seen to come at the cost of innovation and improvement through wider competition.

Attempts have been made to address this challenge through industry initiatives, such as the concept of "fintech passports." The objectives of these initiatives have been to streamline sourcing and procurement processes and create a standardised approach to due diligence. By aligning common requirements across the sector in areas such as vulnerability management, broader security, operational resilience and regulatory compliance, the idea is that smaller providers can satisfy a single, recognised framework, speeding up the ability to contract with large financial institutions.

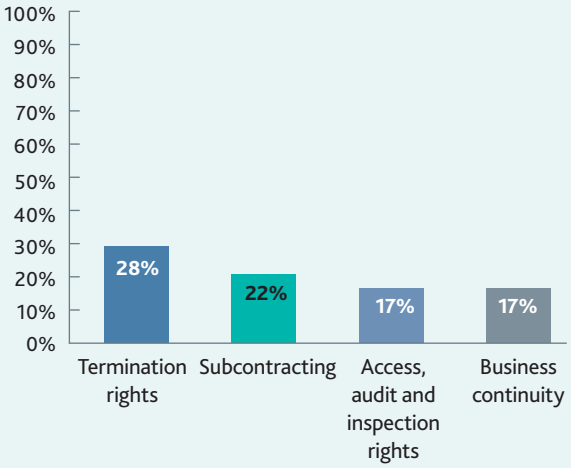
However, in practice, these initiatives have largely failed to achieve broad industry acceptance. Financial institutions therefore continue to rely on their own bespoke and nuanced approaches to due diligence and questionnaires. For young innovative businesses with limited resources, the process of tailoring responses and evidence for each potential client is expensive and time-consuming.

3.4 Opaque contracting and friction points

While major cloud vendors now understand how to meet the regulatory standards required by financial institutions, their complex contracting models remain difficult to navigate according to many of our interviewees. As one adviser to the sector noted, "The issue tends to be that the contract structure is complex, based on having multiple overlapping addenda, schedules and other parts. It becomes a jigsaw puzzle to put together, and also a concern that there will be inadvertent breach due to not fully understanding how the picture fits together. All of this results in additional legal cost."

The market's reliance on a few dominant cloud providers creates concerns around systemic or concentration risk, according to the regulators, which need to be continuously assessed.

Contractual friction points remain



Respondents were asked to rate a list of contractual friction points when procuring cloud or negotiating cloud contracts on a scale of 1 to 5 with 1 representing "unimportant", 4 "important" and 5 "very important". The chart below sets out the total percentage of respondents which selected the following friction points as either important or very important:

Vendor dynamics challenge

The most challenging compliance areas are not broad regulatory principles, but specific contractual and operational clauses. Termination rights lead concerns at **28%**, followed by subcontracting at **22%**. These figures validate the ongoing struggles with exit strategies and the need for greater visibility and control over vendor supply chains – key friction points that persist in cloud contracting negotiations.

4. Future trajectory and emerging issues

The cloud journey is far from over. A new set of strategic issues is emerging that will define the next decade of digital transformation in financial services, moving the focus from foundational adoption to optimisation and sustainability. Beyond this and towards the horizon, industry leaders may anticipate some technological disruptions as well as societal ones, including consumer acceptance and sensitivities to data sharing and security.

4.1 Applying lessons from cloud to AI

The future of AI is inextricably linked to cloud. For most financial institutions, "if they're going to do anything with AI, they have to go to the cloud". The crucial task now is to avoid repeating the mistakes of the early cloud adoption phase. As one executive stated, "we're now on the same journey with Gen AI. We're trying to take those lessons learned from cloud and apply them." This means embedding robust governance, cost control, architectural standards, and data quality management from the outset.

Firms must also anticipate the maturation of AI commercial models. The current phase is characterised by heavy investment and promotional pricing to secure adoption. However, once that adoption is secured and investors demand returns, history suggests the industry will see significant price rises and the emergence of the same lock-in dynamics seen in the cloud market. Applying the lessons of the cloud means planning for this eventuality now.

4.2 Emerging constraints: energy and sustainability

The immense energy consumption of data centres has changed from a not often mentioned ESG concern to a material business issue. The computational demands required to train AI will only intensify this pressure, making the question of "how do we power this" one of the biggest challenges for providers.

While some interviewees feel this issue has become secondary due to recent macroeconomic pressures, there is a recognition that providers with a strong focus on renewable energy are "ahead of the curve" and that sustainability will become a "bigger priority" in the coming years. To put the scale of the challenge into perspective, data centres and data transmission networks already account for approximately 1-1.5% of global electricity use according to some reports, a figure that is projected to grow significantly. According to the International Energy Agency, overall data centre electricity consumption could reach over 1,000 TWh by 2026 under a high-growth scenario which is roughly equivalent to the entire current electricity consumption of Japan.

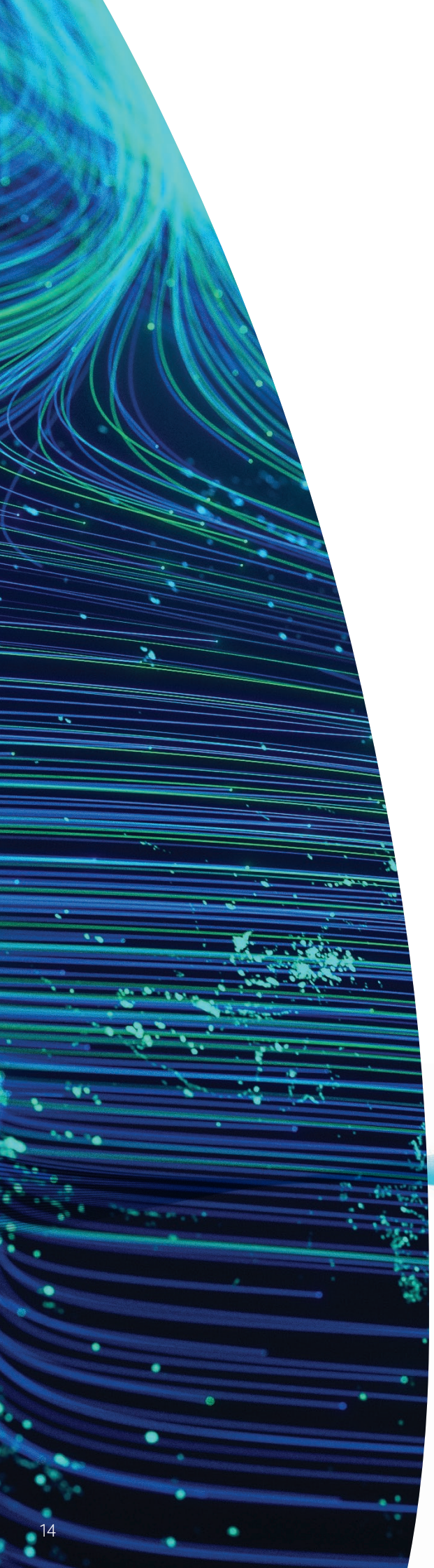
Leading cloud service providers are pursuing sustainability initiatives, which many see as a key competitive differentiator. Many are entering into long-term Power Purchase Agreements (PPAs) to fund new renewable energy projects, such as wind and solar farms, to match their consumption. Innovation in data centre design is also crucial. Providers are focused on improving their Power Usage Effectiveness (PUE), a metric that measures how efficiently a data centre uses energy. For financial services firms, a provider's verifiable commitment to renewable energy and operational efficiency is becoming an important component of procurement and third-party risk management.

The sheer scale of future power requirements, however, is leading some industry leaders to propose more radical solutions. Highlighting this point, Jensen Huang, the CEO of chip manufacturer Nvidia, recently suggested that the UK is having a "goldilocks" moment when it comes to AI, but "It's just missing the infrastructure". Some commentators have said that the computational power needed for a nationwide AI infrastructure would be so vast that the existing National Grid may not be able to accommodate it without disrupting public supply, underscoring the systemic nature of the challenge ahead. Simply buying renewable energy may not be enough; a fundamental rethink of national energy infrastructure may be required to support the digital ambitions powered by cloud.

4.3 The CTP regime: shifting the regulatory burden

A fundamental shift in the regulatory landscape is underway with the introduction of oversight regimes for CTPs in the UK and EU. The current model, where regulators approach "individual financial institutions and ask them about their use of cloud," is seen as a "real drain" and an "incredibly difficult, time-consuming expensive " process for firms to manage.

The prospect of regulators directly supervising the critical third parties (CTPs) themselves is widely welcomed. One leader predicted that the "entire financial services industry would collectively give a sigh of relief" if direct oversight reduced the overall compliance and documentation burden for all involved. If it is effective in shifting a significant portion of the compliance burden onto the vendors, who will be held to account directly, it may also have the benefit of improving the quality of compliance within the sector. As another interviewee argued, there is "absolutely a role for the cloud services providers in playing a bigger part of making the regulators' jobs easier."



These new CTP oversight regimes promise to reshape the dynamics of risk, responsibility and regulation, marking the next major evolution in the financial services cloud journey. However, the regulators have also been clear – their oversight of CTPs is not intended to in any way diminish the accountability of regulated entities.

From a contractual perspective, CTPs face new challenges as they look to ensure that their customers are not impeding their ability to meet the CTP's own regulatory duties. In the UK, for example, CTPs will need to ensure that their customer contracts do not prevent them from dealing with the regulators in an open and cooperative way and disclosing to each regulator anything relating to the CTP of which it would reasonably expect notice. CTPs will also need to ensure that they flow down obligations to their subcontractors to ensure that the CTP's ability to comply with their regulatory obligations is fully supported. CTPs may also have more focus on customer dependencies in contracts, where failure by the customer to meet the dependency could materially impact resilience and lead to enforcement action against the CTP.

4.4 Paving the way for future technologies

A mature cloud infrastructure is increasingly seen as a prerequisite for adopting next generation technology. As many industry analyses highlight, cloud platforms provide the only viable access model for extraordinarily capital-intensive fields like quantum computing. For financial services, this means the cloud investments made now are foundational for maintaining a competitive technological edge in the future, enabling access to complex modelling and computational capabilities that would be impossible to build in-house.

> **From a contractual perspective, CTPs face new challenges as they look to ensure that their customers are not impeding their ability to meet their own regulatory duties.**

5. The way forward

A decade ago, the "cloud in financial services" conversation was framed by caution, with the sector focused on navigating a series of hurdles to adoption. Today, cloud is no longer a novel proposition cautiously assessed but rather an indispensable component of the operational fabric and strategic future of financial services. The hurdles have, in many respects, become pathways, enabling unprecedented speed and innovation.

This transition, however, has revealed a more complex and challenging landscape than was first envisioned. The perception of risk has flipped: where security was once the primary barrier, the resilience offered by hyperscalers is now a core driver.

Yet, the early promise of simple cost savings has proven illusory, and the industry continues to grapple with the immense challenge of "building the plane while it's flying" by retrofitting governance onto rapidly adopted technology.

Persistent issues of vendor lock-in, supply chain opacity, and the stubborn complexities of data residency and legacy integration remain significant drags on progress.

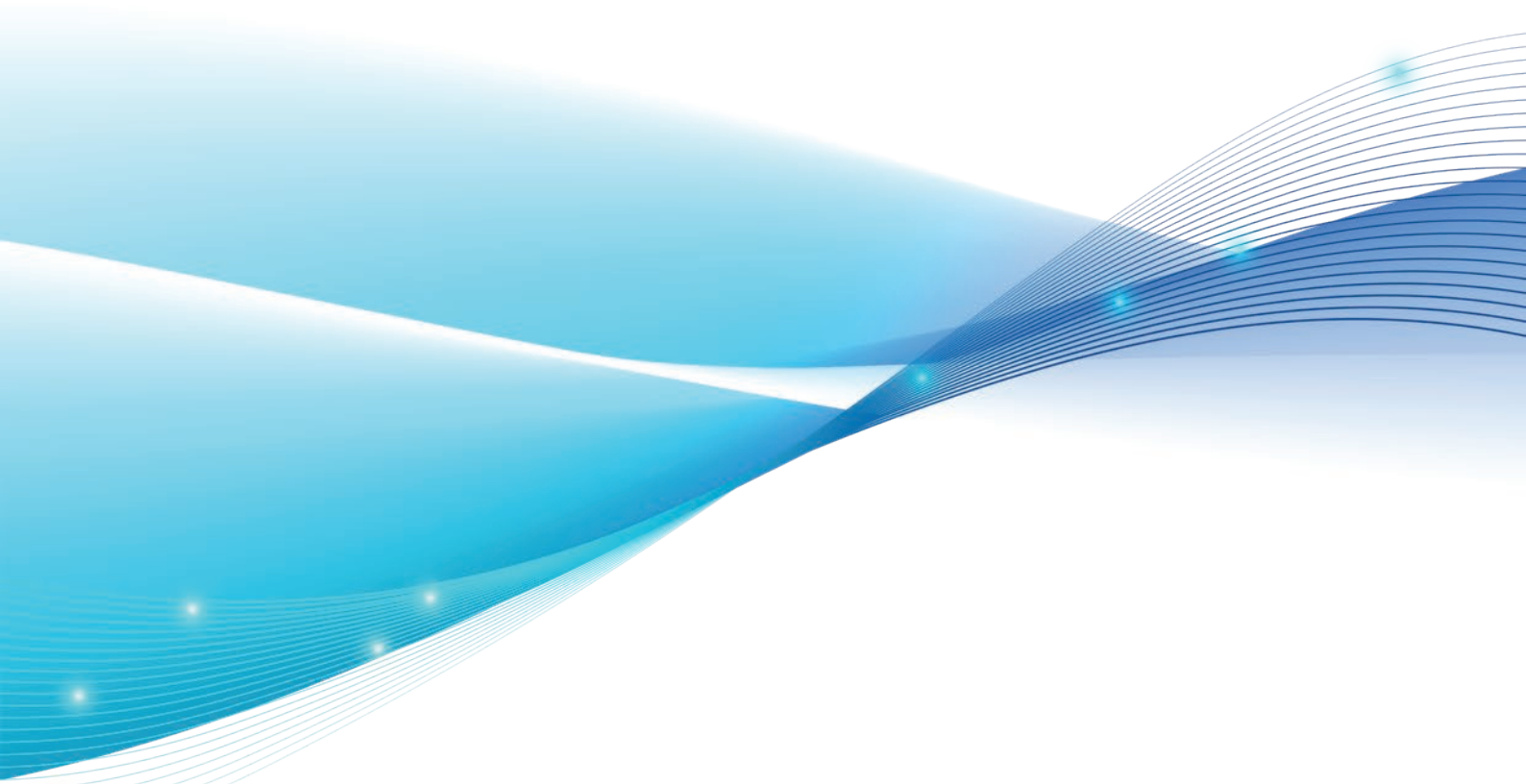
A new technological wave powered by AI is here, and it is inextricably dependent on the cloud. The success of this next iteration will hinge on the industry's ability to apply the hard-won lessons of its cloud journey.

Looking ahead, the regulatory landscape is set for its own transformation. The emergence of direct oversight for critical third parties will lead to change, potentially shifting a portion of the compliance burden directly onto the major vendors. Ultimately, the story of cloud in financial services is a lesson in transformation itself. The greatest challenges were never about the technology, but about regulatory compliance, governance, culture, and the organisational will to move beyond legacy. Mastering these human and strategic elements will be the defining factor for success in the decade to come.

To continue the conversation on cloud, please contact us:

Yvonne Dunn
Partner, Head of financial services technology
+44 (0)141 249 5460
+44 (0)7917 173 269
yvonne.dunn@pinsentmasons.com

Luke Scanlon
Head of fintech propositions
+44 (0)20 7490 6597
+44 (0)7887 815 950
luke.scanlon@pinsentmasons.com



1934877